مجلة جامعة دمشق للعلوم القانونية

اسم المقال: المعالجة الإلكترونية للبيانات الشخصية بين قدسية الخصوصية والحماية الجزائية
اسم الكاتب: عيسى مد الله المخول
رابط ثابت: https://political-encyclopedia.org/index.php/library/10358
تاريخ الاسترداد: 2026/11/01 05:50 +03

الموسوعة السياسيّة هي مبادرة أكاديمية غير هادفة للربح، تساعد الباحثين والطلاب على الوصول واستخدام وبناء مجموعات أوسع من المحتوى العلمي العربي في مجال علم السياسة واستخدامها في الأرشيف الرقمي الموثوق به لإغناء المحتوى العربي على الإنترنت.
لمزيد من المعلومات حول الموسوعة السياسيّة - Encyclopedia Political، يرجى التواصل على info@political-encyclopedia.org

استخدامكم لأرشيف مكتبة الموسوعة السياسيّة - Encyclopedia Political يعني موافقتك على شروط وأحكام الاستخدام المتاحة على الموقع https://political-encyclopedia.org/terms-of-use

تم الحصول على هذا المقال من موقع مجلة جامعة دمشق للعلوم القانونية ورفده في مكتبة الموسوعة السياسيّة مستوفياً شروط حقوق الملكية الفكريّة ومتطلبات رخصة المشاع الإبداعي التي ينضوي المقال تحتها.

مجلة جامعة دمشق للعلوم القانونية
المجلد 5 (3) – 2025: 287-316

Damascus University Journal of Legal Sciences Vol 5
(3) -2025: 287-316

المعالجة الإلكترونية للبيانات الشخصية بين قدسية الخصوصية والحماية الجزائية

عيسى مد الله المخول[1*]

[1] * أستاذ كلية الحقوق، جامعة دمشق، دكتوراه دولة في القانون الجزائي والعلوم الجنائية من جامعة ليون الثالثة (جان مولان) في فرنسا. issaalmakhoul@damascusuniversity.edu.sy

الملخص:

البيانات مورد لا يقل ولا ينضب تتزايد دوماً ولا تتناقص بالاستخدام أو تستهلك، وهي في الحقبة المعاصرة مصدر قوة اقتصادية وسياسية لمن يحسن جمعها وتنسيقها واستخدامها.

ترتبط هذه البيانات بمختلف مجالات النشاط الإنساني وتداخل في كل جوانب الحياة المعاصرة مما جعل توفيرها وحسن استغلالها من المقومات الضرورية لدفع عجلة التقدم في الأمم والمجتمعات، وصار تدفقها وانسيابها بمثابة العصب لجهد التنمية والتحديث والرقي الحضاري وبات الوعي بأهميتها مظهراً ومقياساً لتقدم الدول. ومع تقدم الجنس البشري بمرور الزمن وازدياد عدد سكان الأرض بدأت البيانات المتداولة تتزايد بقفزات واسعة وطرأ على رصيدها الكلي طفرة كمية فاقت طاقة الفكر الإنساني على متابعتها أولاً بأول والاستفادة منها بالدرجة المطلوبة وإزاء هذه الطفرة بدت الطرق التقليدية لجمع وتنظيم البيانات الشخصية عاجزة عن تلبية حاجات التقدم المجتمعي، وأصبح محتماً استخدام أساليب علمية وتقنية متطورة لمواجهة فيض هذه البيانات والتعامل معه. ومن هنا بدأ استخدام وسائل تقانة المعلومات كتقنية متقدمة في التحكم بالبيانات وتجميعها ومعالجتها وتخزينها واسترجاعها والانتفاع بها. وأصبح مألوفاً نقل هذه البيانات عبر الشبكات الإلكترونية، وغدا العالم أشبه بمجتمع كبير تترابط فيه وسائل تقانة المعلومات ومختلف شبكات الاتصال، وتتدفق بين أرجائه البيانات الشخصية.

الكلمات المفتاحية: المعالجة الإلكترونية، الحماية الجزائية.

تاريخ الايداع: 2024/12/15
تاريخ القبول: 2025/1/7

حقوق النشر: جامعة دمشق – سورية، يحتفظ المؤلفون بحقوق النشر بموجب
CC BY-NC-SA

ISSN: 2789-7621 (online)
https://journal.damascusuniversity.edu.sy

Electronic processing of personal data between the sanctity of privacy and criminal protection

Issa Madallah ALMAKHOUL*[1]

[1*] Professor and Head of the Department of Criminal Law, Faculty of Law, University of Damascus, State Doctorate in Criminal Law and Criminal Sciences from university of Lyon III (Jean Moulin) in France.

issaalmakhoul@damascusuniversity.edu.sy

Received: 15/12/2024
Accepted: 7/1/2025

Copyright: Damascus University- Syria, The authors retain the copyright under a CC **BY- NC-SA**

Abstract:

Information technology has begun to be used as an advanced technology in controlling, collecting, processing, storing, retrieving and making use of data. It has become commonplace to transfer this data via electronic networks, and the world has become more like a large society in which means of information technology and various communication networks are interconnected, and personal data flows between its parts.

Accordingly, information technology and communication networks contain a huge amount of personal data, and in this huge environment, monitoring and control are weakened, which increases the risks of attacking this data. Consequently, electronic progress and increasing reliance on information technology means to manage societal affairs have been accompanied by risks based on illegal access to personal data and its misuse, which affects the privacy of individuals.

This research is related to studying the penal policy adopted by the Syrian legislator in protecting personal data through Law No. 12 of 2024 regarding the protection of personal data, and the extent of divergence and convergence between the basis of penal protection stipulated in this law, and the protection of data through other laws, the most important of which is the law regulating Communication on the network, combating cybercrime, and the Civil Status Law, let us reach the end of our research to determine the suitability of the Syrian legislator's penal policy in achieving adequate protection for this data in a way that ensures preserving the sanctity of people's privacy.

Key Words: Electronic processing, Criminal Protection.

المقدمة:

البيانات مورد لا يقل ولا ينضب تتزايد دوماً ولا تتناقص بالاستخدام أو تستهلك، وهي في الحقبة المعاصرة مصدر قوة اقتصادية وسياسية لمن يحسن جمعها وتنسيقها واستخدامها.

ترتبط هذه البيانات بمختلف مجالات النشاط الإنساني وتداخل في كل جوانب الحياة المعاصرة مما جعل توفيرها وحسن استغلالها من المقومات الضرورية لدفع عجلة التقدم في الأمم والمجتمعات، وصار تدفقها وانسيابها بمثابة العصب لجهد التنمية والتحديث والرقي الحضاري وبات الوعي بأهميتها مظهراً ومقياساً لتقدم الدول (رستم، 1992، ص 2). ومع تقدم الجنس البشري بمرور الزمن وازدياد عدد سكان الأرض بدأت البيانات المتداولة تتزايد بقفزات واسعة وطرأ على رصيدها الكلي طفرة كمية فاقت طاقة الفكر الإنساني على متابعتها أولاً بأول والاستفادة منها بالدرجة المطلوبة (خليفة، نيسان 1984، ص 12). وإزاء هذه الطفرة بدت الطرق التقليدية لجمع وتنظيم البيانات الشخصية عاجزة عن تلبية حاجات التقدم المجتمعي، وأصبح محتماً استخدام أساليب علمية وتقنية متطورة لمواجهة فيض هذه البيانات والتعامل معه. ومن هنا بدأ استخدام وسائل تقانة المعلومات كتقنية متقدمة في التحكم بالبيانات وتجميعها ومعالجتها وتخزينها واسترجاعها والانتفاع بها. وأصبح مألوفاً نقل هذه البيانات عبر الشبكات الإلكترونية، وغدا العالم أشبه بمجتمع كبير تترابط فيه وسائل تقانة المعلومات ومختلف شبكات الاتصال، وتتدفق بين أرجائه البيانات الشخصية.

وبناءً على ذلك تذخر وسائل تقانة المعلومات وشبكات الاتصال بكم هائل من البيانات الشخصية، وفي هذه البيئة الضخمة تضعف المراقبة والتحكم مما يرفع من مخاطر الاعتداء على هذه البيانات. وبالتالي فقد جاء التقدم الإلكتروني وتزايد الاعتماد على وسائل تقانة المعلومات في تسيير شؤون المجتمع مصحوباً بمخاطر تقوم على الوصول غير المشروع للبيانات الشخصية، وإساءة استخدامها مما يؤثر على خصوصية الأفراد.

ومع إدراك خطورة وسهولة الاعتداء على البيانات الشخصية والتنبه لآثاره السلبية على جهود التنمية الإدارية والاجتماعية والاقتصادية بدأت مكافحتها تحظى باهتمام متزايد من الحكومات، وأخذ الفنيون وخبراء الأمن السيبراني يركزون جهودهم العملية على سد الثغرات في المنظومات المعلوماتية وتحسين وتطوير أساليب الحماية الفنية للبيانات الشخصية لتصل إلى أقصى درجة ممكنة من الفعالية دونما إنكار من جانبهم للحاجة للقانون لإسباغ صفة عدم المشروعية على الاعتداء على البيانات الشخصية. **(سري طه**، 1988، ص 64).

استناداً إلى كل هذه الاعتبارات أصدر المشرع السوري القانون رقم 12 لعام 2024، الذي سيعدُّ نافذاً اعتباراً من 2025/1/1، والذي يهدف إلى ضمان الحماية القانونية للبيانات الشخصية للأفراد وحماية خصوصيتهم، وتحديد حقوق والتزامات كافة الأطراف لجهة جمع البيانات ومعالجتها، وإلزام المؤسسات والجهات والأفراد المتحكمين في البيانات الشخصية أو المعالجين لها بتعيين مسؤول لحماية البيانات الشخصية داخل مؤسساتهم وجهاتهم، بما يضمن خصوصية بيانات المواطنين السوريين بصيغتها الإلكترونية المنشورة على الشبكة، وتنظيم آلية تبادل البيانات محلياً أو عبر الحدود مع الدول التي يتم إجراء اتفاقيات متبادلة معها ضمن شروط خاصة وبموافقة صاحب البيانات، ووضع آلية تقديم الطلبات والشكاوى من قبل أصحاب البيانات التي تمَّ انتهاكها دون إذن من صاحبها.

أهمية البحث:

تكمن أهمية هذا البحث في التوجه الواضح الذي سلكته الجهورية العربية السورية في الاعتماد على وسائل تقانة المعلومات وشبكات الاتصال في تحقيق التنمية والتقدم في مختلف قطاعات المجتمع، مما يجعل من الضروري الاهتمام بدراسة سلبيات ومخاطر هذه التقنيات، وفي مقدمتها المخاطر على البيانات الشخصية حتى يمكن تقليل هذه المخاطر أو تفاديها إن أمكن.

إشكالية البحث:

تتمثل إشكالية هذا البحث في دراسة السياسة الجزائية التي اعتمدها المشرع السوري في حماية البيانات الشخصية من خلال القانون رقم 12 لعام 2024 الخاص بحماية هذه البيانات، ومدى التباعد والتقارب بين أساس الحماية الجزائية المنصوص عليها في هذا القانون، وبين حماية البيانات من خلال قوانين أخرى ومن أهمها قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية وقانون الأحوال المدنية، لنصل في نهاية بحثنا لتحديد مدى ملائمة السياسة الجزائية للمشرع السوري في تحقيق حماية كافية لهذه البيانات بما يضمن الحفاظ على قدسية خصوصية الأشخاص؟

مخطط البحث:

المبحث الأول: ماهية حق خصوصية البيانات الشخصية المعالجة إلكترونياً.

المطلب الأول: الطبيعة القانونية للحق

المطلب الثاني: نطاق تطبيق الحق

المبحث الثاني: أسس الحماية الجزائية للبيانات الشخصية المعالجة إلكترونياً.

المطلب الأول: تعدد أسس القواعد التجريمية الناظمة لحماية البيانات الشخصية .

المطلب الثاني: تفريد القواعد العقابية الناظمة لحماية البيانات الشخصية.

المبحث الأول:

ماهية حق خصوصية البيانات الشخصية المعالجة إلكترونياً:

تعدُّ وسائل تقانة المعلومات من أخطر آلات التكنولوجيا المعاصرة تهديداً لحق خصوصية البيانات، كيف لا وهي الوسائل التي بواسطتها أصبح للجهات العامة والخاصة الحق في أن تجمع وتخزن كل ما يخص الفرد من معلومات، مما يجعله مجرداً من جميع السواتر أمام هؤلاء جميعاً. من هنا كان لابد لرجال القانون من التصدي لمفهوم حق خصوصية البيانات في علاقته مع وسائل تقانة المعلومات، وهذا ما سنعالجه في هذا الفصل حيث نبين الطبيعة القانونية لهذا الحق، ثم نوضح نطاق تطبيقه.

المطلب الأول:

الطبيعة القانونية للحق:

نتناول في هذا المطلب التعريف بالأساس القانوني لحماية هذا الحق جزائياً، وأسباب هذه الحماية، ولكن قبل التعرف على طبيعته القانونية، لابد من توضيح ما المقصود من هذا الحق.

الفرع الأول:

مفهوم الحق:

نبين في هذا الفرع التعريف الفقهي لهذا الحق، ثم نوضح تعريفنا له، والنتائج التي نستخلصها من هذا التعريف.

أولاً : تعريف حق خصوصية البيانات الشخصية المعالجة إلكترونياً:

قام العديد من الفقهاء بالتعبير عن المقصود بحق خصوصية البيانات الشخصية المعالجة إلكترونياً إلا أنّ الكلمات التي أطلقها السيد جون فريس وهو المدير العام لمجلس التحريات الخاصة بالمعلومات في السويد تعتبر من أهم ما قيل في هذا الحق : "*إن المشكلة الكبرى أن العالم لم يتعلم كيف يتداول البيانات مع احترام حقوق الإنسان*" (J.BUTZ, 2019 , p. 67). كما أن عدة آراء قانونية أشارت في معرض إبراز ضرورة حماية حق خصوصية البيانات المعالجة إلكترونياً إلى أن أهمية وسائل تقانة المعلومات فاقت كل شيء، لذلك فالسؤال ليس هو هل نقوم بتخزين البيانات الشخصية واستخدامها إنما هو كيف يمكن أن نفعل ذلك بشكل مشروع ؟.

وفي هذا الصدد أبرز الأستاذ ألين ويستن معنى هذا الحق حينما قال بأنه: " *حق الأفراد والمجموعات والمؤسسات أن يحددوا لأنفسهم متى وكيف وإلى أي مدى يمكن للبيانات الخاصة بهم أن تصل للآخرين*". (**المقاطع** ، 1992 ، ص 41)

وقد عرفته الأستاذة لورا كلوكي بأنه : " *حق الفرد في أن يضبط عملية جمع البيانات الشخصية عنه وعملية معالجتها إلكترونياً وحفظها وتوزيعها واستخدامها في صنع القرار الخاص به أو المؤثر عليه* ". (المقاطع، 1992، ص 43). وفي الصدد ذاته ذكر الأستاذ فرويسني:

"*لا وجود اليوم لحرية رفض إعطاء البيانات الشخصية، ولكن بدلاً من ذلك فإن الحرية استقرت في القدرة على السيطرة على هذه البيانات التي أدخلت إلى وسائل تقانة المعلومات، وبناء على ذلك فهناك الحق في الوصول إلى بنوك البيانات والحق في تحديثها وتصحيحها والحق في سرية البيانات الحساسة والحق في السماح بنشرها، وجميع هذه الحقوق اليوم تشكل ما يسمى حق خصوصية البيانات الشخصية بمفهومه الجديد* " . (علي، 2009، ص 120).

ومن الواضح هنا أن الأستاذ فرويسني إنما يميل إلى ترجيح اعتبار حق خصوصية البيانات الشخصية المعالجة إلكترونياً حقاً موحداً ، وإن كان ينطوي على العديد من الحقوق التي تعتبر مهمة له لأن كل واحد منها يحقق السيطرة على البيانات والتي هي هدف حق خصوصية البيانات.

ومن خلال ما سبق يمكن أن نصل إلى تعريف حق خصوصية البيانات الشخصية المعالجة إلكترونياً بأنه: **حق دستوري يخول الأشخاص سواء أكانوا طبيعين أم اعتباريين العديد من الضمانات لحماية البيانات الشخصية في مواجهة معالجتها إلكترونياً ضماناً لحريتهم واستقلالهم في الوسط المحيط بهم.**

من خلال تحليل التعريف الذي توصلنا إليه أعلاه يمكن أن نستنتج الآتي:

1 . إن حق خصوصية البيانات الشخصية المعالجة إلكترونياً هو حق دستوري، أي أن الأساس القانون لهذا الحق لابد أن يكون منصوصاً عليه في الدستور، وهذا ما سنبحثه في الفرع الثاني.

2 . إن نطاق حماية هذا الحق لابد أن تشمل كل من الأشخاص الطبيعيين والأشخاص الاعتباريين، وهذا ايضاً ما سنبحثه في الفرع الثاني.

والجدير بالذكر أن المشرع السوري اعترف في دستور الجهورية العربية السورية الصادر في عام 2012 بالمكانة السامية للحق في الحياة الخاصة، وجرم كل شكل من أشكال المساس بها حيث نصت **المادة 54 منه** على أن: "*كل اعتداء على الحرية الشخصية أو **على حرمة الحياة الخاصة**، أو على غيرها من الحقوق والحريات العامة التي يكفلها الدستور يعد جريمة يعاقب عليها القانون*".

ثانياً: الضمانات المستخلصة من حق خصوصية البيانات الشخصية المعالجة إلكترونياً:

تكمن العلّة في إعطاء ضمانات للشخص الذي تتم معالجة بياناته الشخصية إلكترونياً بالخوف من أماكن تخزينها لدى الجهات المختلفة ألا وهي بنوك البيانات ؟ ويقصد بتلك البنوك الحاسبات التي تتمتع بقدرة فائقة على تجميع أكبر قدر من البيانات من مصادر مختلفة وتخزينها واسترجاعها في وقت قصير، بالإضافة إلى قدرتها على عمل فهارس وبطاقات لهذه البيانات وتنظيمها، بحيث تعطي في النهاية صورة متكاملة عن الشخص. فمن خلال ذلك يمكن لنا أن ندرك مدى الخطورة المترتبة على اختراق هذه البنوك حيث يتمكن المعتدي من البحث عن البيانات التي يريدها والوصول إليها والاطلاع عليها ونسخها بسهولة وفي أسرع وقت ممكن.

وقد حدد القانون رقم 12 لعام 2024 الأشخاص الذين يحق لهم إنشاء هذه البنوك وسماهم المتحكم والمعالج. **حيث عرفت المادة الأولى** من هذا القانون المتحكم بأنه شخص طبيعي أو اعتباري يكون له بحكم عمله الحق في الحصول على البيانات الشخصية وتحديد طريقة وأسلوب ومعايير الاحتفاظ بها أو معالجتها والتحكم فيها طبقاً للغرض المحدد أو نشاطه. **في حين عرفت المادة ذاتها** المعالج بأنه شخص طبيعي أو اعتباري يختص بحكم عمله بمعالجة البيانات الشخصية لصالحه أو لصالح المتحكم بالاتفاق معه ووفقاً لتعليماته.

إن حق خصوصية البيانات الشخصية المعالجة إلكترونيا يمنح الشخص العديد من الضمانات لحماية بياناته ومنها:

1 . حق الاحتفاظ : يعتبر هذا الحق من أهم الضمانات التي أعطيت للشخص في مواجهة تدخل الدولة في شؤونه الخاصة، وعملاً به فإن للشخص أن يحتفظ لنفسه بجميع البيانات التي تتعلق به، وأن يرفض إعطاء أي بيانات عنه، وهذا هو المبدأ العام، فالشخص حر في ألا يعلم الناس أو الجهات العامة أو الخاصة عنه أي شيء، طالما أنه لا يوجد نص قانوني معين يلزمه بإعطاء البيانات. (**عباس** ، 1995، ص 92). ويعدُّ حق الشخص في الاحتفاظ ببياناته من الحقوق الجوهرية الضامنة لخصوصية معلوماته، ومن ثم وجب الاعتراف به وتأكيده تشريعياً بما يساعد الشخص على تحقيق استقلاله الشخصي من تدخلات الآخرين ومضايقاتهم، ولقد أطلق المفكر الإنكليزي جون ستيوارت ميل مقولته الشهيرة حول هذا الموضوع: "*إن الإنسان له سيطرة كاملة على نفسه وجسده وعقله*". (**مغبغب**، 1998، ص 30).

وهذا ما نص عليه القانون رقم 12 لعام 2014 حيث نصت الفقرة أ من المادة 3 على حظر معالجة البيانات الشخصية أو الإفصاح عنها أو إفشاؤها إلا بموافقة صريحة من صاحب البيانات أو في الأحوال المصرح بها قانوناً.

2 . حق الإخطار : لابد أن يعترف للشخص بحق الإخطار من قبل الجهة المخزنة لبيانات تتعلق به، فالشخص ربما لا يكتشف مطلقاً بأن هناك بيانات تخصه معالجة إلكترونيا، لذلك فإنه لابد من أن يعلم ذلك، وليس هذا فحسب بل يجب أن يعرف وبشكل مفصل عن ماهية ونوعيه هذه البيانات لكي يتمكن من تصحيحها إن كانت خاطئة، مما يقلل من إمكانية الإساءة إليه. ويرى الأستاذ ويستن أنه :

" عندما يعرف الشخص صاحب البيانات أن الشخص المسؤول عن حفظ البيانات سوف يخطره لمعرفة ما هو مدون عنه، وأنه يستطيع الاعتراض على إساءة استخدام هذه البيانات فإن ذلك يعتبر ضمانة كبيرة لحماية البيانات من سوء استخدامها ". (الفحل، 1995، ص 672).

وهذا ما نص عليه القانون رقم 12 لعام 2014 حيث نص البند 1 من الفقرة ب من المادة 3 عندما أعطى الحق لصاحب البيانات في العلم بطبيعة بياناته الشخصية موضوع المعالجة، والغاية منها وطرقها والحقوق التي يضمنها له القانون.

3 . حق الاطلاع : ويعني هذا الحق أنه يمكن للشخص أن يطلع على البيانات المخزنة عنه، وأن يصل إليها بسهولة دون وضع عوائق في مواجهته إدارية أو مالية. وقد تحدث عن هذا الحق الأستاذ فروسيني عندما قال بأن: *" الحرية اليوم تكمن في القدرة على التحكم بالبيانات الشخصية المخزنة في برامج الحاسوب الآلي"*. (المقاطع، 1992، ص 111)، **وهذا ما نص عليه القانون رقم 12 لعام 2014 حيث نص البند 2 من الفقرة ب من المادة 3** عندما أعطى صاحب البيانات الحق في الوصول إلى بياناته الشخصية الموجودة لدى أي متحكم أو معالج أو الاطلاع عليها أو الحصول عليها.

4 . حق تعديل المعلومات وتصويبها : حيث يحق للشخص الذي علم بأن هناك معلومات عنه لدى إحدى الجهات، سواء أكانت عامة أو خاصة وقام بالاطلاع عليها، أن يطلب من تلك الجهة أن تقوم بتصحيح المعلومات الخاطئة عنه، ويعدل ما يشوبها من مغالطات قد تؤثر على سمعته وتسبب له خسائر لا سبيل لتجنبها. ولابد من الإشارة إلى أنه يجب أن يعطى الشخص حقه في التعديل والتصويب في وقت مبكر ومناسب وقبل أن يضار منها، إذ أن تأخير الشخص من ممارسة هذا الحق إلى ما بعد وقوع الضرر ما يضطره من اللجوء إلى القضاء لاستيفاء حقه. **وهذا ما نص عليه القانون رقم 12 لعام 2014 حيث نص البند 5 من الفقرة ب من المادة 3** على حق صاحب البيانات في تصحيح أو تعديل أو إضافة أو تحديث بياناته الشخصية.

5 . حق معرفة الغرض من جمع البيانات وتخزينها: فيجب أن يحاط الشخص ومنذ اللحظة الأولى لطلب البيانات عنه بالهدف والغاية الأساسية التي سيتم استخدام هذه المعلومات فيها، وله أن يمتنع عن تزويد أي جهة بالبيانات إذا لم تقم بذلك، بل وله ألا يسمح بأن يتم استخدام البيانات المخزنة عنه في غير الأغراض المجمعة من أجلها في الأصل، فضلا عن ضرورة مشروعية الغرض الذي سيتم استخدام البيانات فيه. وانطلاقاً من ذلك فقد قضت المحكمة الدستورية في ألمانيا بأنه لا حرية رأي أو حرية اجتماع والحرية مؤسسات يمكن أن تمارس كاملة ما دام الشخص غير متيقن في ظل أي ظروف ولأجل أي هدف جمعت عنه البيانات الشخصية وعولجت إلكترونياً. (علي، 2009، ص 129)، **وهذا ما نص عليه القانون رقم 12 لعام 2014 حيث نص البند 1 من الفقرة ب من المادة 3** على حق صاحب البيانات في العلم بالغاية من معالجة بياناته الشخصية.

6 . حق تقديم شكوى : قد يفاجأ الشخص في أحيان كثيرة بأن بعض الجهات قد أصدرت قرارات ضارة بمصلحته، لذلك يحق له أن يسلك كل الطرق المشروعة والممكنة كي يتحرى عن البيانات الشخصية التي لدى هذه المؤسسة، والتي استندت إليها في إصدار قرارها ، ويحق له أن يطلب من أي جهة حائزة لبيانات عنه أن تزوده بنسخة منها وأن يتقدم بشكوى على هذه الجهة . **وهذا ما نص عليه القانون رقم 12 لعام 2014 حيث نص البند 9 من الفقرة ب من المادة 3** على حق صاحب البيانات في تقديم شكوى إلى هيئة حماية البيانات الشخصية.

7 . حق توقيت تخزين البيانات : ويعني هذا الحق بأنه لابد من وضع مدة محددة يجوز أثنائها فقط للجهة الحائزة لبيانات شخصية أن تحتفظ بها، أي أنه لا يجوز لها أن تبقى حائزة لمثل هذه البيانات لمدة غير محددة وهذا الأمر يتطلب ما يلي:

أن يحدد مع غرض الاستخدام المدة المتوقع أن تنتهي فيها الحاجة لمثل هذه البيانات، ومن جهة أخرى إعطاء الحق للشخص أن يطلب من الجهة المخزنة لمعلومات عنه بضورة إنهاء حيازتها لهذه المعلومات بعد انتهاء المدة المحددة أو بانتهاء الغرض الذي وافق من أجله على إعطائها مثل هذه البيانات.

وهذه الضمانة تعدُّ من الضمانات المهمة التي تساعد الشخص على أن يهنأ بعيشة هادئة وحياة مستقرة دون أن يكون قلق البال، ولفترة قد تمتد طوال حياته. **وهذا ما نص عليه القانون رقم 12 لعام 2014 حيث نص البند 3 من الفقرة ب من المادة 3** على حق صاحب البيانات من معرفة الفترة الزمنية التي تخزن فيها البيانات الشخصية أو بالمعايير المستخدمة لتحديدها، كما نص البند 6 من الفقرة و من المادة ذاتها على حق صاحب البيانات في تخصيص معالجة بياناته لغايات محددة أو في نطاق محدد.

8 . حق استرداد المعلومات: ويعني هذا الحق أن يعطى الشخص القدرة في أن يسترد ما سبق وأن أعطاه من بيانات عنه لإحدى الجهات عندما يخشى الإساءة إلى وضعه وسمعته[1]. **(مغبغب، ص 247)، وهذا ما نص عليه البند رقم 4 من الفقرة ب من المادة 3** من القانون رقم 12 لعام 2024 عندما أعطى الحق لصاحب البيانات بالعدول عن الموافقة المسبقة على الاحتفاظ ببياناته الشخصية أو معالجتها دون أن يكون لذلك العدول مفعول رجعي.

9 . حق المحو والإلغاء : ففي حال وجود بيانات خاطئة عن الشخص فيجب منحه الحق في أن يطلب محو هذه البيانات المخزنة عنه بل يجوز له ذلك حتى ولو كانت هذه البيانات صحيحة ولكنها أصبحت غير ذي فائدة وتحمل أضرار محققة على مصالحه. **(المقاطع ، 1992 ، ص 118)، وهذا ما نص عليه البند رقم 4 من الفقرة ب من المادة 3** من القانون رقم 12 لعام 2024 عندما أعطى الحق لصاحب البيانات الشخصية في محو هذه البيانات.

10ـ الحق بعدم تسجيل معلومات شخصية حساسة : وذلك كالمعلومات الدينية أو الطائفية أو الحزبية أو السياسية حتى ولو رضي الشخص بتخزينها لأن تجميع مثل هذه المعلومات وتخزينها في وسائل تقانة المعلومات قد تنزل أضراراً جسيمة بالأشخاص في حال تم إساءة استعمالها لاحقاً. (السيد، 1983، ص 577).

وقد عرف القانون رقم 12 لعام 2024 البيانات الشخصية الحساسة في المادة الأولى منه بأنها: "*أي بيانات تفصح عن الصحة النفسية أو العقلية أو البدنية الجينية أو بينات القياسات الحيوية البيومترية أو البيانات المالية أو المعتقدات الدينية أو الآراء السياسية أو الحالة الجنائية أو بيانات الأطفال وفاقدي الأهلية*". **وقد حددت المادة 13 من القانون ذاته** القواعد الخاصة بمعالجة هذه البيانات الحساسة حيث حظرت على المتحكم أو المعالج معالجة هذه البيانات الشخصية الحساسة إلا بترخيص أو تصريح من هيئة حماية البيانات الشخصية، كما يجب الحصول على موافقة كتابية وصريحة من صاحب البيانات عدا الأحوال المصرح بها قانونا. وفي حال إجراء أي معالجة لبيانات تتعلق بالأطفال فيتوجب أخذ موافقة النائب الشرعي.

الفرع الثاني:

التأصيل القانوني للحق:

إن تحديد الأساس القانون لحق خصوصية البيانات الشخصية المعالجة إلكترونياً إنما يستند في الأصل إلى الأساس الذي بموجبه تم الاعتراف للأشخاص بالخصوصية وسنبين في هذا الفرع ما هو هذا الأساس؟ وماهي الأسباب التي دعت لحماية هذا الحق بذلك الأساس ؟

1

أولاً: الأساس القانوني لحق خصوصية البيانات الشخصية المعالجة إلكترونياً:

إن الأساس الذي يعدُّ منطلق هذا الحق هو الحقوق الدستورية اللصيقة بالشخصية الإنسانية، إذ أن حق خصوصية البيانات الشخصية المعالجة إلكترونياً ليس إلا أحد هذه الحقوق، وبالتالي فإن الدستور هو الحامي والأساس لهذا الحق.

ومما يؤيد ذلك ويدعمه الأحكام القضائية الصادرة في العديد من الدول، فقد أصدرت المحكمة الاتحادية العليا في الولايات المتحدة الأمريكية حكماً قررت فيه أن حق خصوصية البيانات حق دستوري مستخلص من وثيقة حقوق الإنسان. وقد شددت هذه المحكمة على أنه بالرغم من عدم ذكر هذا الحق في الدستور، إلا أن التمتع بالحقوق التي تحميها وثيقة حقوق الإنسان العالمية يقتضي تأكيد حق خصوصية البيانات باعتباره من الحقوق الدستورية. (المقاطع، 1992، ص 36).

كما أن الجمعية العامة للأمم المتحدة في قرارها رقم 23/2450 لعام 1989 أوحت بلزوم الإعداد لدستور عالمي لحماية حقوق الإنسان ضد الأخطار المترتبة على التطور العلمي والتكنولوجي ، أي أنه لا يمكن توفير الحماية القانونية الكافية إلا عن طريق دستور دولي يؤكد عدم استخدام التكنولوجيا في إلحاق الضرر بحقوق الإنسان الشرعية. **(عباس**، 2009، ص 96).

بناءً على ما تقدم يمكن لنا أن نخلص إلى أن الأساس القانوني الذي يستمد منه الشخص الضمانات التي تمكنه من حماية بياناته الشخصية المعالجة إلكترونياً والذود عنها في مواجهة أي نوع من أنواع التعرض أو الاعتداء عليها إنما يستند إلى أن حق خصوصية البيانات الشخصية المعالجة إلكترونياً يعد أحد أهم الحقوق الدستورية.

ثانياً: الحكمة من اعتبار حق خصوصية البيانات الشخصية المعالجة إلكترونياً حقاً دستورياً:

إن السؤال الذي يطرح هنا لماذا يتوجب التأكيد على اعتبار حق خصوصية البيانات الشخصية المعالجة إلكترونياً حقاً دستوريا ؟ إن الإجابة على هذا التساؤل تكون من خلال التعرف على المخاطر الكبيرة التي قد يسببها انتهاك هذا الحق، والتي قد تؤدي إلى تدمير حياة الشخص الذي تتعلق به هذه البيانات مما استدعى بالضرورة حماية قوية له، وهل من حماية أقوى من حماية الدستور وهو الحامي الأساسي لحريات الأشخاص والضامن الأكبر لحقوقهم. **(القايد**، 1988، ص 77).

وسنعرض الآن لأهم المخاطر التي يسببها الاعتداء على هذا الحق:

1 . تجاوز استعمال البيانات الشخصية المخزنة للغرض المقصود منها : إن نوع وحجم البيانات التي يعطيها الشخص عن نفسه تختلف باختلاف الهدف الذي دفعه إلى إعطاء تلك البيانات، وبالتالي فإن من أبلغ المخاطر التي تصيب حق خصوصية البيانات الشخصية المعالجة إلكترونياً هي استخدام تلك البيانات استخدامات عديدة تتجاوز الهدف الذي جمعت عنه في الأساس، فمثلا إذا كان الهدف من جمع البيانات هو الإحصاء فلا يجوز استعمالها بالتالي لأغراض ضريبية لأنها قد تلحق الضرر بالشخص. **(مغبغب**، 1998، ص 242) وهنا يبرز التساؤل التالي: إذا تبين للدولة فيما بعد أن هذا الاستخدام كان في محله فهل من مسؤولية على الجهة المعالجة للبيانات الشخصية عن هذا التجاوز في استخدام البيانات ؟

إن هذه الجهة تكون مسؤولة عن استخدام البيانات في أغراض تجاوز الهدف الذي جمعت من أجله سواءً كان هذا الاستخدام في محله أم في غير محله وذلك للأسباب الآتية:

* إن هذه الجهة في هذه الحالة تخدع الأشخاص الذين قبلوا إعطاء البيانات عنهم لغرض محدد، فإذا بها تستعملها لأغراض أخرى لو علموا بها مسبقاً لما قبلوا إعطاء هذه البيانات .

* يجب على الدولة أن تسعى للتعرف على مخالفة الأشخاص للقوانين والأنظمة النافذة بالطرق القانونية المشروعة، وأن لا تلجأ إلى الأساليب غير المشروعة لكشف هذه المخالفات.

* إن قيام هذه الجهة بهذا التجاوز تضعف الثقة بينها وبين الأشخاص المتعاملين معها، مما يدفعهم إلى التهرب من إعطائها بيانات عنهم في الأحوال الأخرى.

انطلاقاً من ذلك **فقد نص القانون رقم 12 لعام 2024 في المادتين 5 و 6** على مجموعة من الالتزامات على المتحكم والمعالج تحد من تجاوز استعمال البيانات الشخصية المخزنة للغرض المقصود منها وهي: عدم إتاحة البيانات الشخصية أو نتائج المعالجة إلا في الأحوال المصرح بها قانوناً، عدم نقل البيانات الشخصية إلى الغير دون إعلام صاحب البيانات، إثبات أن صاحب البيانات قد وافق على معالجة بياناته الشخصية عندما تعتمد المعالجة على الموافقة، محو البيانات الشخصية لديه فور انقضاء الغرض المحدد منها، أما في حال الاحتفاظ بها لأي سبب من الأسباب المشروعة بعد انتهاء الغرض فيجب ألا تبقى في صورة تسمح بتحديد صاحب البيانات، والتأكد من طبيعة وصحة البيانات الشخصية واتفاقها مع الغرض المحدد لجمعها وكفايتها له، عدم إجراء أي معالجة للبيانات الشخصية تتعارض مع غرض أو نشاط المتحكم، وعدم تجاوز الغرض المحدد للمعالجة ومدتها.

2 . الدخول غير المرخص به إلى البيانات الشخصية: ويمكن تصور هذا الخطر في صور عديدة منها أن يحصل شخص على كلمة السر للملفات التي تخزن فيها البيانات الشخصية المعالجة إلكترونياً فهنا ينتهك أمن البيانات مما يؤدي إلى التسلل إلى هذه الملفات والاطلاع عليها وإخراج ما فيها من بيانات عن الأشخاص، وهذا يستوجب أن تكون وسائل تقانة المعلومات المخزنة فيها البيانات مشتملة على مواصفات معينة تمنع تعرضها لأي مخاطر مثل الوصول غير المصرح به للبيانات الشخصية. **(الفيومي،** 2000، ص 1240).

انطلاقاً من ذلك فقد **نص القانون رقم 12 لعام 2024 في المادتين 5 و 6** على مجموعة من الالتزامات على المتحكم والمعالج تضمن عدم الدخول غير المشروع إلى هذه البيانات ومن ذلك: وجوب اتخاذ الإجراءات التقنية والتنظيمية وتطبيق المعايير القياسية المعتمدة من قبل هيئة حماية البيانات الشخصية لحماية هذه البيانات وتأمينها حفاظاً على سريتها وسلامتها، ومسك سجل خاص يتضمن على الأقل وصف فئات البيانات الشخصية لديه وتحديد من سيفصح لهم عن هذه البيانات أو يتحيها لهم وسنده والمدة الزمنية وقيودها ونطاقها وآليات محو البيانات الشخصية لديها أو تعديلها، وأي بيانات أخرى متعلقة بنقل تلك البيانات الشخصية عبر الحدود، ووصف الإجراءات التقنية والتنظيمية الخاصة بأمن البيانات .

3 . فقدان الشخص لحقوق متعددة : لما كانت البيانات التي تؤخذ عن شخص معين تخزن في وسائل تقانة المعلومات فإنها دون شك عرضة لمجموعة من الأخطاء الفنية من جهة والأخطاء الاعتيادية من جهة أخرى (الفحل، ص 673)، إلا أن الأمر الذي يلاحظ أن مجرد وجود خطأ في البيانات المخزنة لن تضر الشخص في حقه في خصوصية بياناته فحسب بل سيفقد إلى جانب ذلك حقوقا أخرى، مثل حقه في العمل أو حقه في الدعم الحكومي أو الضمان الصحي، فعلى سبيل المثال عندما تتم معالجة معلومات ناقصة أو غير صحيحة عن شخص، فإنه في حال تقدم للحصول على الدعم الحكومي في السلع الأساسية فإنه قد يفاجأ برفض طلبه رغم أنه شخصياً يجزم باستحقاقه لمثل هذا الدعم في حين أن الجهة العامة استندت في هذا الرفض إلى ما هو متوافر لديها من بيانات شخصية خاطئة أسس عليها قراراها. **(المقاطع،** *1992*، ص 101) انطلاقاً من ذلك فقد **نص القانون رقم 12**

لعام 2024 في المادة 5 أنه يتوجب على المتحكم أن يضمن إمكانية تحديث أو تصحيح اي خطأ بالبيانات الشخصية فور إبلاغه أو علمه بها.

4 . التشهير والإساءة إلى السمعة : إن رضاء الشخص في أن تخزن بيانات معينة عنه إلكترونياً يعني أنه استودع سره لدى جهة من الجهات التي يعتقد أنه لن يضار منها سواء بالإساءة إلى شخصه أو بتعكير صفو حياته. غير أن هذا الاعتقاد وإن صدق إلى درجة كبيرة في أحوال عديدة إلا أن الشخص لا يزال معرضاً لمخاطر عديدة قد تعرضه للتشهير وإلى نشر ما لا يرغب أن يعرفه الناس عنه حتى لو كانت هذه البيانات صحيحة، إذ أن مجرد نشر بيانات من هذا النحو تكفي لأن تجعله قضية تداولها الألسن، ويساء إليه من خلالها، مما يجعل سمعته عرضة للتجريح والأقاويل التي هو في غنى عنها. **(المقاطع**، *1992*، ص 102) ولذلك **نصت الفقرة الرابعة من المادة التاسعة من القانون رقم 12 لعام 2024** على ضرورة تعيين مسؤول لدى الجهة التي تتولى معالجة البيانات يتولى حماية البيانات، وأنه يجوز لصاحب البيانات درءاً لإساءة استعمال هذه البيانات الاتصال بمسؤول حماية البيانات فيما يتعلق بجميع القضايا المتعلقة بمعالجة بياناته الشخصية.

5 . الضغط والابتزاز السياسي : لم يعد غريباً اليوم أن نسمع بأن شخصاً قد اضطر إلى الخضوع إلى تهديدات معينة بالرغم من أنه شخص قوي الشخصية وذات مكانة اجتماعية رفيعة، والسر في هذا قد يرجع إلى أن من قام بعملية ابتزازه أو الضغط عليه استطاع أن يصل ويحوز بيانات معالجة إلكترونياً عنه فيعمد إلى استعمال هذه البيانات للضغط عليه بصور من الصور، (سلبي، 2021، ص 56، الرواشدة، 2022، ص 69) مما يؤدي إلى كسر الحصن المنيع للشخص الذي يدرأ به عن نفسه ما لا يتوقعه من المخاطر ألا وهو حصن خصوصية البيانات. (الفحل، 1995، ص 672).

المطلب الثاني:

نطاق تطبيق الحق:

نتناول في هذا المطلب موضوعاً مهماً من موضوعات حق خصوصية البيانات الشخصية المعالجة إلكترونياً وهو بيان وتحدي الأمور التي يشملها حماية هذا الحق، وتدخل ضمن حدوده وتتمتع بحصانته، وعليه سنوضح نطاق تطبيق هذا الحق من حيث الأشخاص الذين تشملهم الحماية، ومن حيث الموضوعات التي تدخل ضمن حمايته.

الفرع الأول:

نطاق تطبيق الحق من حيث الأشخاص:

ندرس في هذا الفرع مسألة يمكن بلورتها على شكل فكرة عامة مؤادها السؤال التالي: هل حق خصوصية البيانات الشخصية المعالجة إلكترونياً يشمل في نطاقه كل من الأشخاص الطبيعية والأشخاص الاعتبارية ؟

أولاً : الشخص الطبيعي: لا خلاف بين الفقه والقضاء في أن الشخص الطبيعي يتمتع بحق خصوصية البيانات الشخصية المعالجة إلكترونياً فهذا الحق نشأ ليكون قلعة وملاذاً للفرد في مواجهة جميع الأمور التي تعكر صفو حياته.

وقد ذهبت بعض الدراسات القانونية إلى اعتبار هذا الحق حق للأشخاص الطبيعية فقط دون غيرهم من الأشخاص لأنهم فقط من تتعلق بهم البيانات الشخصية ولا يشمل ذلك الأشخاص الاعتبارية. **(الشهاوي**، 2005، ص 308، **حسان**، 2001، ص 273).

وجاءت التشريعات لتدعم هذا الاتجاه فعلى سبيل المثال فإن قانون حماية البيانات الانكليزي لعام 1984 قد وضع تعريفا ضيقاً لمن يخضع للحماية فقصره على الشخص الطبيعي دون الشخص الاعتباري، فالبيانات التي يحميها هذا القانون هي تلك التي تتعلق

بالفرد باعتباره كائناً حياً، والذي يمكن أن يعرف من خلال هذه البيانات. **(رستم،** *1992*، ص 359) وقد سار على هذا النهج ذاته الاتفاقية ألأوروبية لحماية البيانات لعام 1980 حيث أبرزت هذه الاتفاقية المقصود من هذا الحق ، وأن مشتملاته إنما تشير فقط لحماية الشخص الطبيعي في مختلف بياناته. **(حسان،** 2001، ص 275 ، **رستم،** *1992*، ص 359**)**

ولم يخرج المشرع السوري عن هذا الاتجاه في **القانون رقم 12 لعام 2024 حيث قصر الحماية على الشخص الطبيعي فقط حينما عرف البيانات الشخصية في المادة الأولى منه** بأنها: " معلومات متعلقة بشخص طبيعي محدد مباشرة أو يمكن تحديده على نحو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخرى كالاسم أو الصوت أو الصورة أو رقم تعريفي أو محدد إلكتروني للهوية أو أي بيانات تحدد حالة الشخص الطبيعي ". كما عرف صاحب البيانات في المادة ذاتها بأنه: " شخص طبيعي تدل عليه بيانات شخصية معالجة تمكن من تمييزه من غيره".

ولابد من الإشارة إلى أن المشرع السوري قصر نطاق الحماية على البيانات العائدة للمواطنين السوريين فقط المنشورة على الشبكة، وهذا ما نصت عليه الفقرة ج من المادة الثانية من القانون رقم 12 لعام 2024 التي ألزمت المتحكمين والمعالجين للبيانات الشخصية باتخاذ التدابير اللازمة بما يضمن خصوصية بيانات المواطنين السوريين بصيغتها الإلكترونية المنشورة على الشبكة. وهذا يدل على أن نطاق هذه الحماية لا يشمل خصوصية البيانات ذاتها العائدة للمواطنين الأجانب. وبمفهوم المخالفة فإن البيانات الشخصية غير المنشورة على الشبكة تكون محلاً للحماية سواء أكانت للمواطنين السوريين أم للمواطنين الأجانب.

ثانياً: الشخص الاعتباري: إن السؤال الذي لا مفر من البحث فيه هو هل الحق في خصوصية البيانات الشخصية المعالجة إلكترونياً لا يزال قاصرا على الأشخاص الطبيعية دون الأشخاص الاعتبارية؟

كادت جميع الدراسات الفقهية أن تقصر هذا الحق على الأشخاص الطبيعية إلى أن تدخل الأستاذ ألين ويستن الذي جاء بتعريف لهذا الحق يشمل في مفهومه الأشخاص الاعتبارية بالإضافة للشخاص الطبيعية حيث ابتدأ بتعريف هذا الحق: " *حق الأفراد أو المجموعات أو المؤسسات....*" **(حسان،** *2001*، ص 277، **رستم،** 1992، ص 359**)**، وقد توالت الآراء القانونية المؤيدة لوجهة النظر التي ترى ضرورة إدخال الأشخاص الاعتبارية ضمن نطاق حق خصوصية البيانات الشخصية المعالجة إلكترونياً، وتتلخص حججهم بالحجتين الآتيتين: فمن جهة أولى إن البيانات التي تعطى عن الأشخاص الاعتبارية تعني كشف بيانات عن مالكي هذه الأشخاص والمسيطرين عليها مما يوجب حمايتها خشية الإضرار بمصالح هؤلاء المالكين، ومن جهة أخرى إن الأشخاص الاعتبارية لها حق مشروع بحماية البيانات التي تتضرر مادياً من الكشف عنها بنفس المنطق الخاص بالأفراد، فالشخص الطبيعي والشخص الاعتباري يشتركان في حاجتهما لحماية بياناتهما.

وقد أيدت العديد من الدول الأوروبية هذا الاتجاه حيث تبنت نصوصاً في قوانينها الخاصة بحماية خصوصية البيانات تعمد إلى حماية كل من الشخص الطبيعي والشخص الاعتباري، ومن هذه الدول النرويج والنمسا وإيرلندا والدنمارك واللكسمبورغ، ففي هذه الأخيرة مثلاً نجد أن القانون رقم 29 لعام 1979 المتعلق بحماية خصوصية البيانات يتضمن نصاً يعرف فيه الشخص في معرض تطبيق هذا القانون بأنه أي شخص طبيعي أو مؤسسة عامة أو خاصة أو جمعية أو مجموعة من الأشخاص.

وقد أشار بعض الكتاب (المقاطع، 1992، 70) إلى أن الأصل أن نطاق حق خصوصية البيانات الشخصية المعالجة إلكترونياً يتقرر للأشخاص الطبيعية، واستثناء وفي ظل شروط محددة يمكن أن يمتد هذا النطاق ليدخل ضمنه الأشخاص الاعتبارية، ويعللون رأيهم بأنه لا يمكن أن نمنح للأشخاص الاعتبارية حقاً في خصوصية البيانات مثل الحق الذي يتمتع به الأشخاص

الطبيعية، وذلك لأن هذا الحق هو بطبيعته من الحقوق اللصيقة بالشخصية والملازمة للطبيعة الإنسانية وهذا هو الأساس الذي نشأ هذا الحق ليرعاه، والسبب الأساسي في التحفظ على مدّ نطاق حق خصوصية البيانات الشخصية إلى الأشخاص الاعتبارية هو كونها تنشأ وفقاً لنظام قانوني محدد، لذلك فإن حماية بياناتها لابد وأن تنظم في ذلك النظام، ومن ثم يسهل عليها إضفاء الحماية اللازمة وفقاً للطبيعة التي تتميز بها وبشكل يتناسب معها من حيث الجزاءات التي لابد وأن تحمى بها.

إلا أن هذا المبدأ لا يمنع البتة من أن يتمتع الشخص الاعتباري بنص خاص وبصفة استثنائية بالحماية القانونية استناداً لحق خصوصية البيانات الشخصية المعالجة إلكترونياً كما هو بالنسبة للأفراد وذلك بتوافر شرطين: الأول أن يؤدي الكشف عن بيانات الشخص الاعتباري إلى التعرف على البيانات الشخصية للأشخاص القائمين على إدارة الشركة أو المسهمين في أنشطتها أو عن مالكيها، والثاني: انعدام أي وسيلة أخرى لحماية البيانات الشخصية المتعلقة بالشخص الاعتباري.

ثالثاً : الرأي الراجح:

بعد هذا العرض للآراء التي عارضت امتداد نطاق هذا الحق ليشمل الأشخاص الاعتبارية والآراء التي أيدت هذا الامتداد يبدو مهماً التعرف على الرأي الراجح.

بالنظر للآراء السابقة يمكن لنا التوصل إلى النتيجة الآتية: إن حق خصوصية البيانات الشخصية المعالجة إلكترونياً يجب أن يشمل في نطاقه كلاً من الأشخاص الطبيعية والأشخاص الاعتبارية وذلك للأسباب الآتية:

1 . امتدت المسؤولية الجزائية لتطال إضافة للشخص الطبيعي الشخص الاعتباري، حيث أصبح هذا الشخص يتعرض للعقاب عند مخالفته وخرقه لنصوص القانون، وأصبح على الشخص الاعتباري التقيد بالواجبات التي تفرضها عليه القوانين والأنظمة كما يتقيد بها الشخص الطبيعي (**العوجي**، 1990، ص 303) وبالتالي فإن من المنطق إذاً أن تمنح للشخص الاعتباري الحقوق التي يتمتع بها الشخص الطبيعي وأن يحميها القانون، ومن هذه الحقوق حق خصوصية البيانات الشخصية المعالجة إلكترونياً.

2 . إذا أمعنا النظر في الكثير من المخاطر التي يمكن أن يتضرر منها الشخص الطبيعي نتيجة لخرق حق خصوصية البيانات الشخصية المعالجة إلكترونياً فإننا سنلاحظ أنها يمكن أن تصيب الشخص الاعتباري وأن يتضرر منها.

3 . إن ترك البيانات الشخصية المعالجة إلكترونياً والمتعلقة بالأشخاص الاعتبارية دون حماية فهذا لا يعرض فقط هذه الأشخاص للخطر بل قد يعرض الاقتصاد الوطني للخطر، وذلك لأن هذه الأشخاص هي الشركات والمؤسسات التي يقوى اقتصاد الدولة بقوتها ويضعف بضعفها، فإذا ما تسربت بيانات عنها إلى جهات معادية فإن هذا سوف يعرضها للخطر الكبير، وبالتالي قد يتعرض الاقتصاد الوطني تبعاً لذلك لأضرار كبيرة .

4. إن الاعتداء على حق خصوصية البيانات الشخصية المعالجة إلكترونياً والمتعلقة بالشخص الاعتباري ليس سوى اعتداء على الشخص الطبيعي المالك للشركة أو المؤسسة لأن الإضرار بالشخص الاعتباري سوف يتحمل نتائجه الشخص الطبيعي المالك لها.

الفرع الثاني:

نطاق تطبيق الحق من حيث الموضوع:

قمنا في الفرع السابق بتحديد الأشخاص الذين تشملهم الحماية المقررة لحق خصوصية البيانات الشخصية المعالجة إلكترونياً، أما في هذا الفرع فإننا سنحدد البيانات التي تدخل ضمن الحماية المقررة لهذا الحق، وعليه فإن دراستنا لهذه البيانات يمكن أن نحددها بأمور مختلفة تبدأ بالبيانات الفردية فالمعلومات المدنية ، بالإضافة إلى البيانات المالية ومعلومات السيرة الاجتماعية والصحية.

أولاً : البيانات الفرديـة: تعبر المعلومات المتعلقة بالشخص ذاته كالصفات التي تحدده وتعرف الناس به بشكل مستقل من أول الموضوعات وأهمها التي يمتد إليها نطاق تطبيق حق خصوصية البيانات الشخصية المعالجة إلكترونياً ولكن السؤال هو ما المقصود من المعلومات الفردية ؟

عرفت لجنة "ليندوب" الإنكليزية البيانات الفردية بأنها: " أي بيانات تتصل بأي شخص خاضع لنظام البيانات يومكن التعرف عليه من خلالها، أو يمكن أن تؤدي إلى معرفته بما في ذلك البيانات التي يمكن أن يعرف بواسطتها " (R. ANDERSON, 2012, p. 56) وتطبيقاً للتعريف السابق يعتبر اسم الشخص وصورته وجنسيته وفصيلة دمه ومحل سكنه أو عمله ورقم هاتفه من البيانات الفردية التي تحظى بالحماية القانونية. ومن البيانات الفردية التي ثار نزاع حول حمايتها الاسم فقد انقسم الفقه حول موضوع حماية الاسم فذهب الاتجاه الأول إلى أن الاسم هو أحد عناصر الحق في الخصوصية الواجب حمايتها، ويستند هذا الرأي إلى أن الشخص يملك حق التمتع بالخصوصية فلا يجوز كشف اسمه إلا برضاه (R. LINODON, 1974, p. 17). بينما اتجه الرأي الثاني إلى أن اسم الشخص ليس عنصراً من عناصر الحق في الخصوصية ولا يجوز حمايته إلا باعتباره محلاً لجرم انتحال الهوية أو الاحتيال (J. ANTONIO, 1976, p.165) ويميل الرأي الراجح إلى عدّ الاسم من ضمن البيانات التي يمتد إليها نطاق الحماية للبيانات الشخصية المعالجة إلكترونياً. **وهذا ما انتهجه المشرع السوري عندما عدّ الاسم من ضمن البيانات الشخصية وفقاً للتعريف الوارد في المادة الأولى من القانون رقم 12 لعام 2024.**

ثانياً: البيانات المدنية: يقصد بالبيانات المدنية عناصر الحالة المدنية للشخص وهي الميلاد والزواج والطلاق والجنسية والوفاة ورقمه الوطني، وليس هناك شك في أن هذه البيانات يسعى الشخص إلى إبعادها عن أنظار وتناول الغير لما لمثل هذه البيانات من حساسية بالغة لو عرفت عنه، حيث أنها ستقيد حركته في المجتمع خصوصاً إذا كانت هذه البيانات مخزنة في وسائل تقانة المعلومات وسهلة التداول دون ضمانات قانونية، وهو أمر يشكل عنصر تضييق وتقليل من انطلاقات الشخص وإبداعه ومشاركته في شؤون الحياة العامة. وقد عدَّ المشرع السوري الرقم التعريفي أو المحدد الإلكتروني للهوية من البيانات الشخصية **وفقاً للتعريف الوارد في المادة الأولى من القانون رقم 12 لعام 2024.**

ثالثاً: البيانات المالية : تعدُّ البيانات المتصلة بالشؤون المالية للشخص من البيانات المهمة التي يمتد إليها نطاق حق خصوصية البيانات المعالجة إلكترونياً، وإذا بحثنا في هذه الشؤون فإنه يندرج تحتها دخل الفرد الشهري وإنفاقه والديون التي له أو عليه أو سمعته المالية لدى المصارف وشركات التأمين وميزانية الشركات أو المؤسسات وخسائرها وأرباحها.

ويلعب الحاسوب دوراً بارزاً في التأثير على شؤون الشخص المالية من جوانب عدة تبلغ ذروتها في حال تداول البيانات المالية عنه آلياً بين عدة مجموعات، حيث يصبح الشخص في وضع لا يحسد لأنه يغدو شخصاً مكشوف الأسرار بمجرد الضغط على زر معين لدى أي من الجهات التي تعالج بياناته الشخصية إلكترونياً. ولهذا السبب **عدّ المشرع السوري وفقاً للفقرة الأولى من القانون رقم 12 لعام 2024 البيانات المالية من البيانات الشخصية الحساسة.**

رابعاً: بيانـات السيرة الاجتماعيـة والصحية: وهي البيانات المتعلقة بمكانة الشخص وارتباطاته وعلاقاته وأوساطه الاجتماعية والعائلية، ويدخل ضمن هذه البيانات سيرة الشخص الصحية وشؤونه السياسية.

وقد أبدى بعض الكتاب قلقهم من المعلومات الصحية المعالجة إلكترونياً خصوصاً في حالة كان الشخص مريضاً فإنه سيكون في حالة مكشوفة أمام شركات التأمين التي تتحفظ على التعامل معه، وهو أمر سيجعل الأطباء يترددون كثيراً في تقديم الرعاية الطبية له، ومن ثم تقليل فرص العلاج الأفضل للشخص المريض.

ولذلك عدَّ المشرع السوري وفقاً للمادة الأولى من القانون رقم 12 لعام 2024 البيانات الصحية أو المتعلقة بالمعتقدات الدينية أو الآراء السياسية من البيانات الشخصية الحساسة.

المبحث الثاني:

أسس الحماية الجزائية للبيانات الشخصية:

بعد التعرف في المبحث الأول على ماهية حق خصوصية البيانات الشخصية المعالجة إلكترونياً، سننتقل في المبحث الثاني لتحليل أساس الحماية الجزائية للبيانات الشخصية المعالجة إلكترونياً، وذلك من خلال بيان تعدد أسس القواعد التجريمية الناظمة لحماية هذه البيانات، وبعد ذلك التعرف على تفريد القواعد العقابية الناظمة لحماية البيانات الشخصية.

المطلب الأول:

تعدد أسس القواعد التجريمية الناظمة لحماية البيانات الشخصية:

تعددت القواعد التجريمية التي تنص على حماية البيانات الشخصية المعالجة إلكترونياً، فإضافة لما نص عليه القانون رقم 12 لعام 2024 في الفصل الرابع عشر منه، فقد تضمن قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم 20 لعام 2022، وقانون الأحوال المدنية رقم 13 لعام 2021 مجموعة من الجرائم التي تعدّ البيانات الشخصية محلاً لها.

الفرع الأول:

حماية البيانات الشخصية في القانون رقم 12 لعام 2024:

حدد القانون رقم 12 لعام 2024 مجموعة من المعايير والضوابط لجمع ومعالجة البيانات الشخصية والاحتفاظ بها، وفرض في الفصل الرابع عشر مجموعة من العقوبات في حال مخالفة هذه المعايير والضوابط. وفي هذا الفرع الأول سنحلل السياسة الجزائية العامة لحماية البيانات الشخصية المعالجة إلكترونياً، والسياسة الجزائية الخاصة لحمايتها.

أولاً: السياسة الجزائية العامة لحماية البيانات الشخصية:

إن تحليل السياسة الجزائية العامة التي اتبعها المشرع السوري في حماية البيانات الشخصية استناداً للقانون رقم 12 لعام 2024 تستوجب التعرف على محل الجريمة، والمصلحة المحمية، ومشروعية إتاحة البيانات الشخصية.

1 . المصلحة المحمية:

تعدُّ فكرة المصلحة المحمية أو الحق المعتدى عليه أحد الأسس المهمة التي يصاغ بموجبها النموذج القانوني للجريمة. وتتنوع المصالح المحمية في التشريع الجزائي إلا أنه لا يمكن النظر إليها على أنها في مستوى واحد أو أنها لا تخضع للمعايرة من حيث ترتيب الأهمية، فمن بين أولى الحقوق التي يجب حمايتها هو حق الدولة في الاستقرار والأمان من العدوان الداخلي والخارجي

وحماية المؤسسات العامة، وحق الأفراد في الحياة والسلامة الجسدية والملكية، وحق المجتمع في حماية الآداب والأخلاق العامة والأسرة والصحة العامة[2]. (المخول، الجريمة الإلكترونية، 2024، ص 51).

ومن الطبيعي أن لا يتمكن التشريع الجزائي من وضع هذه الحقوق والمصالح في مستوى واحد، مما يعني أن عملية وضع النموذج القانوني للجريمة تتطلب دراسة الواقع الاجتماعي والقيم والأولويات التي يقدرها عموم أبناء المجتمع، وهذه الأمور متغيرة من مكان إلى آخر ومن زمن إلى آخر، وكم من التشريعات الإصلاحية العظيمة فشلت وسقطت عند محاولة تنفيذها لأنها لم تأخذ بالاعتبار القيم الاجتماعية السائدة، فالأفكار العظيمة لا تكفي لوحدها بل ينبغي أن تكون وسائل تنفيذها ملائمة، وأن لا توقع صدمة في مشاعر أبناء المجتمع نتيجة انهيار القيم المفاجئ، فلدى البشر عداء تاريخي وحذر دائم من التغييرات المفاجئة.

ولذلك شغل تحديد مفهوم المصلحة المحمية جانباً كبيراً من دراسة الفلاسفة، فيرى الفيلسوف الإيطالي بكاريا بأن المصلحة يجب أن تستند إلى فكرة المنفعة العامة كأساس للتشريع الجزائي فيقول: "*إن فكرة المنفعة العامة تكون مزيفة حينما تأخذ في الاعتبار المحاذير الخاصة قبل المحاذير العامة*[3]" (T.GARE, , 2022, p. 57)، ويرى الفليسوف روسكوباوند في قراءة متعمقة في نظرية المصالح بأن: "*الظروف الاجتماعية التي يتكفل القانون بحمايتها لا تقتصر على القيم المادية ، بل تشمل القيم المعنوية*[4] ". (***المخول***، *الجريمة الإلكترونية*، 2024، ص 52).

وفي إطار القانون الجزائي تختلف المصالح حسب أهميتها، ويستهدي المشرع بمجموعة من المعايير حين يضع حماية لمصلحة معينة أو حين يفضلها على مصالح أخرى، وهذه المعايير هي المعيار التاريخي ومعيار التناسب والمعيار المنطقي والمعيار العملي. (R.VITU, 1981 , p. 23)

إن هذه المعايير تحدد الوسيلة التي يستخدمها المشرع الجزائي في عملية تقييم وتبني المصلحة أو إسباغ حماية أكبر لمصلحة معينة وتقديمها وتفضيلها على مصالح اخرى أقل أهمية منها، وإن كل معيار بمفرده لا يصلح أساساً لتقييم المشرع لمصلحة وتبنيها دون أخرى أو تفضيلها أو تقديمها عليها.

وفي إطار قانون حماية البيانات الشخصية المعالجة إلكترونياً رقم 12 لعام 2024 نجد أن المشرع وضع في نصب عينيه حماية المصلحة الخاصة للفرد في حماية خصوصيته. **ويمكن القول أن المصلحة المحمية في الجرائم الواقعة على البيانات الشخصية المعالجة إلكترونياً هي الحق في المحافظة على خصوصية البيانات الشخصية للأفراد.**

2 . محل الجريمة: تمثل البيانات الشخصية محلاً للجرائم المنصوص عليها في القانون رقم 12 لعام 2024، وقد قسم المشرع السوري هذه البيانات إلى قسمين البيانات الشخصية العادية، والبيانات الشخصية الحساسة. وقد عرفنا هذين النوعين في المبحث الأول من هذه الدراسة. ومن خلال تحليل هذين التعريفين نجد أن المشرع اشترط في البيانات الشخصية لتكون محلاً للجريمة الآتي: فمن جهة أولى لابد أن تتعلق بشخص طبيعي أي بالأفراد، وبالتالي فإن المشرع استثنى من نطاق الحماية الجزائية البيانات المتعلقة بالأشخاص الاعتبارية، حيث لا يمكن أن تكون محلاً للجريمة. ومن جهة ثانية يشترط أن تقود هذه البيانات لتحديد

الشخص إما مباشرة أو على نحو غير مباشر، ومن جهة ثالثة أن تمكن هذه البيانات من تمييز الشخص عن غيره. وهذا الشرط الثالث مستنتج من تعريف **صاحب البيانات المنصوص عليه في المادة الأولى من القانون رقم 12 لعام 2024 .**

3 . مشروعية معالجة البيانات الشخصية : من المعروف أن مبدأ المشروعية يقلب الفعل الجرمي إلى فعل مباح قانوناً، وهذه المشروعية تتكرس من خلال أسباب التبرير (J.PRADEL, 2005, p. 256) ، **وقد نص القانون رقم 12 لعام 2024** على مجموعة من أسباب التبرير الخاصة إضافة لأسباب التبرير العامة التي نص عليها قانون العقوبات، وفي حال توافر إحداها فلا تعدُّ المعالجة فعلاً مجرماً.

وفي تحديد مفهوم المعالجة **نصت المادة الأولى من القانون رقم 12 لعام 2024** على أن المعالجة تعني:

"كل عملية إلكترونية أو تقنية لإدخال البيانات الشخصية بصيغتها الإلكترونية أو تجميعها أو تسجيلها أو حفظها أو تخزينها أو دمجها أو عرضها أو إرسالها أو استقبالها أو تداولها أو نشرها أو محوها أو تغييرها أو تعديلها أو استرجاعها أو تحليلها، وذلك باستخدام أي من الوسائل الإلكترونية سواء تم ذلك بصورة جزئية أم كلية" . **وقد نصت المادة السابعة من هذا القانون** على أن معالجة البيانات الشخصية تعدُّ **مشروعة** في حال توافر إحدى الحالات الآتية وهي: موافقة صاحب البيانات على إجراء المعالجة من أجل تحقيق غرض محدد أو أكثر، تنفيذاً لالتزام تعاقدي أو تصرف قانون أو لإبرام عقد لصالح صاحب البيانات أو لمباشرة أي من إجراءات المطالبة بالحقوق القانونية له أو الدفاع عنها، تنفيذ التزام ينظمه القانون أو تنفيذاً لقرار أو حكم صادر عن السلطة القضائية ، تمكين المتحكم أو المعالج من القيام بالتزاماته ما لم يتعارض ذلك مع حقوق صاحب البيانات، أن تستند إلى بيانات صحيحة ومحدثة، ألا تسبب الضرر لصاحب البيانات أو تنال من حقوقه بشكل مباشر أو غير مباشر، أن تتم بطريقة تضمن سرية البيانات وسلامتها وعدم حدوث أي تغيير عليها.

إن الصياغة التشريعية لهذه المادة تكشف لنا أن توافر حالة واحدة من هذه الحالات تجعل معالجة البيانات الشخصية مشروعة، ولكن من خلال قراءة هذه الحالات سنجد أن هذا الأمر غير دقيق، فهل المعالجة المستندة إلى بيانات صحيحة ومحدثة دون أخذ موافقة صاحب البيانات على إجراء هذه المعالجة تجعل المعالجة مشروعة؟ إن الإجابة بالتأكيد لا. **ولذلك فإننا نجد أن بعض هذه الحالات ليست أسباب تبرير بل هي شروط للمعالجة وليس لمشروعيتها وهناك فارق كبير بين الشروط والمشروعية، فالمشروعية تعني تبرير الفعل المجرم وهذا ما نسميه سبب التبرير وليتحقق سبب التبرير لابد من توافر شروط فيه.** ولتوضيح ذلك نذكر أن رضاء صاحب البيانات بالمعالجة هو سبب تبرير، ولكن هناك شروط للمعالجة وهي أن تستند إلى بيانات صحيحة، وألا تسبب الضرر لصاحب البيانات، وأن تتم بطريقة تضمن سرية البيانات وسلامتها. فهذه الشروط لا يمكن عدّها أسباب تبرير كما فعل المشرع.

ثانياً: السياسة الجزائية الخاصة لحماية البيانات الشخصية:

نص المشرع في المواد من 37 حتى 39 من القانون رقم 12 لعام 2024 على مجموعة من القواعد التجريمية والعقابية لحماية البيانات الشخصية، **مكرساً في المادة 37 مجموعة من الجرائم والعقوبات وفي المادة 38 نصاً خاصاً للعقاب على الشروع ، وفي المادة 39 نص على عقوبة إضافية.**

1 . الجرائم والعقوبات:

قسم المشرع الجرائم التي تهدف إلى حماية البيانات الشخصية إلى قسمين: **القسم الأول: يشترط توافر ركن مفترض في مقترف هذه الجرائم بأن يكون فاعل الجريمة معالجاً أو متحكماً، أما القسم الثاني فلم يشترط في توافر الركن المفترض.**

أ . القسم الأول : نص المشرع في المادة 37 في الفقرات أ ، د، هـ، من القانون رقم 12 لعام 2024 على مجموعة من الجرائم التي يقترفها المعالج أو المتحكم ، **حيث نصت الفقرة أ** على إيقاع عقوبة الحبس من شهر إلى ستة اشهر وبغرامة من مليون إلى ثلاثة ملايين ليرة سورية كل من معالج أو متحكم جمع بيانات شخصية دون توافر المعايير المنصوص عليها في المادة الرابعة، وهي : أن تجمع البيانات الشخصية لأغراض مشروعة ومحددة ووفقاً للسبل المتاحة في هذا القانون، وأن تعالج بطريقة مشروعة وملائمة للأغراض التي تم تجميعها من أجلها، وألا يتم الاحتفاظ بها لمدة أطول من المدة الزمنية اللازمة للوفاء بالغرض المحدد لها إلا إذا كان الاحتفاظ بها هو لأغراض الأرشفة أو للمصلحة العامة، أو لأغراض البحث العلمي أو التاريخي أو لأغراض الإحصائية، وأن تكون صحيحة وسليمة وتتم معالجتها بطرقة تضمن الأمن المناسب للبيانات الشخصية بما في ذلك الحماية من المعالجة غير المصرح بها أو غير القانونية وضد الفقد أو التلف العرضي وذلك باستخدام التدابير الفنية أو التنظيمية المناسبة.

كما **نصت الفقرة د** على فرض عقوبة الحبس من ثلاثة أشهر إلى سنتين وبغرامة من سبعة ملايين إلى عشرة ملايين ليرة سورية كل متحكم أو معالج لم يلتزم بواجباته بإبلاغ الهيئة فوراً بوجود خرق على البيانات الشخصية وإعلام صاحب البيانات خلال ثلاثة أيام عمل من تاريخ الإبلاغ بما تم اتخاذه من إجراءات.

كما نصت **الفقرة هـ** على فرض عقوبة السجن من ثلاث سنوات إلى سبع سنوات وبغرامة من عشر ملايين إلى عشرين مليون ليرة سورية على اقتراف جريمة إجراء عمليات نقل البيانات الشخصية التي تم جمعها أو تجهيزها للمعالجة أو تخزينها أو مشاركتها إلى دولة عربية أو أجنبية دون التحقق من مستوى الحماية المقبول من الهيئة وبترخيص منها وعلى لجريمة نقل أو مشاركة أو تداول أو معالجة البيانات الخصية إلى دولة دون أن يتوافر فيها مستوى الحماية المقبول من الهيئة. وعلى جريمة إتاحة البيانات الشخصية لمتحكم أو معالج آخر خارج الجمهورية العربية السورية من دون توافر الشروط الآتية: اتفاق طبيعة عمل كل من المتحكمين أو المعالجين أو وحدة الغرض الذي يحصلان بموجبه على البيانات الشخصية، توافر المصلحة المشروعة لدى كل من المتحكمين أو المعالجين للبيانات الشخصية أو لدى صاحب البيانات، وألا يقل مستوى الحماية القانونية والتقنية للبيانات الشخصية لدى المتحكم أو المعالج الموجودة بالخارج عن المستوى المحدد في التعليمات التنفيذية للقانون رقم 12 لعام 2024.

ب . القسم الثاني: نص المشرع **في المادة 37 في الفقرات ب، و، ز،** على مجموعة من الجرائم التي تقترف من أي شخص سواء أكان متحكم أو معالج أو شخص آخر غيرهما.

فقد **نصت الفقرة ب** على فرض عقوبة الحبس من شهر إلى ستة أشهر والغرامة من خمسة ملايين إلى سبعة ملايين ليرة سورية على كل من جمع أو عالج أو أفشى أو أتاح أو تداول أو خزن أو نقل أو حفظ أو حذف بيانات شخصية معالجة إلكترونياً بأي وسيلة من الوسائل دون موافقة صاحب البيانات أو في غير الأحوال المصرح بها قانوناً.

كما نص المشرع في **الفقرة و** على جريمة ممارسة أي عمل من الأعمال المنصوص عليها في هذا القانون والتي تستوجب الحصول على ترخيص أو تصريح من الهيئة قبل الحصول عليه.

في حين نص المشرع في **الفقرة ز** على جريمة منع أو إعاقة أحد العاملين بالهيئة ممن يتمتعون بصفة الضابطة العدلية عن أداء عمله دون عنف بالحبس من شهر إلى ثلاثة أشهر وبغرامة من خمسة ملايين إلى سبعة ملايين ليرة سورية.

ولابد من الإشارة إلى أن المشرع لم ينص على عد إتاحة البيانات الشخصية للغير بشكل غير مشروع جرماً مستقلاً بل جعل المعالجة والإتاحة غير المشروعة يشكلان صوراً للجرم نفسه المنصوص عليه في الفقرة ب من المادة 37 من القانون رقم 12 لعام 2024، على الرغم من اعتبار المشرع لفعل الإتاحة مختلفاً عن فعل المعالجة وفقاً لما ورد في المادة الأولى من القانون رقم 12 لعام 2024 ، حيث عرف المشرع إتاحة البيانات الشخصية في المادة الأولى من هذا القانون بأنها:

" أي وسيلة تحقق وصول الغير إلى البيانات الشخصية كالاطلاع أو التداول أو النشر أو النقل أو الاستخدام أو العرض أو الإرسال أو الاستقبال أو الإفصاح عنها ".

وحيث أن فعل المعالجة أشد خطورة من فعل الإتاحة، وذلك كون صور السلوك الجرمي التي يتضمنها تعريف المعالجة أشد جسامة، وخاصة أفعال تجميع وحفظ وتسجيل هذه البيانات، الأمر الذي يستتبع معه ضرورة التفريق بين النموذج القانوني لجرم المعالجة والنموذج القانوني لجرم الإتاحة.

2 . حالات عدم تطبيق القانون رقم 12 لعام 2024:

لا تطبق أحكام القانون رقم 12 لعام 2024 وفقاً لأحكام المادة 40 منه على معالجة البيانات الشخصية والبيانات الشخصية الحساسة في الحالات الآتية:

أ . البيانات التي يحتفظ بها الشخص الطبيعي لصاحب البيانات، والتي يتم معالجتها من قبله في نطاق الأنشطة الشخصية، شريطة عدم الكشف عنها لأي طرف دون موافقة صاحب البيانات، والامتثال للالتزامات المتعلقة بحماية البيانات.

ب . لأغراض الاحصاءات الرسمية التي تجريها الجهات المختصة بذلك قانونياً .

ج . لأغراض إعلامية أو علمية بشرط أن تكون صحيحة ودقيقة، وألا يكون الغرض منها اتخاذ أي قرار أو إجراء أو انتهاك للخصوصية أو الحقوق الشخصية لصاحب البيانات.

د . لأعراض تحقيق متطلبات الأمن الوطني أو النظام العام أو لتحقيق المصلحة العامة أو بهدف منع وقوع جريمة أو كشفها من قبل الجهات المختصة.

هـ . البيانات المتعلقة بمحاضر الضبط القضائي والتحقيقات والدعاوى القضائية.

ي . البيانات التي يتم تبادلها بين الدول أو الوزارات في نطاق الأنشطة الوقائية لمواجهة حالات الكوارث والأوبئة العامة.

ومن الملاحظ أنه في بعض هذه الحالات، التي غابت فيها الحماية الجزائية للبيانات، ستتعرض قدسية خصوصية الأشخاص للخطر، وخاصة في ظل عدم وجود معيار واضح لتفسير مصطلحات النظام العام أو المصلحة العامة الواردة في الفقرة ج من المادة 40 من القانون رقم 12 لعام 2024، الأمر الذي يوجب معه إعادة النظر في تقليص عدد هذه الحالات، وذلك لتأمين حماية جزائية كافية للبيانات الشخصية المعالجة إلكترونياً.

الفرع الثاني:

حماية البيانات الشخصية وفقاً للقانون رقم 20 لعام 2022:

تضمن قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية **رقم 20 لعام 2022** بعض النصوص التجريمية التي تهدف إلى حماية البيانات الشخصية سواء من خلال التعديل أو الحذف أو النسخ.

أولاً: جريمة تجاوز حدود الدخول المشروع:

تنص المادة الحادية عشرة من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية على هذه الجريمة ، حيث تقترف حيث الجريمة بفعل تجاوز حدود الدخول المشروع، ويقصد بذلك أن الجاني قد دخل بشكل مشروع إلى نظام معلومات، أو موقع إلكتروني أو حساب شخصي، وبعد ذلك قام بتجاوز حدود هذا الدخول. وقد **عرفت المادة 11 من التعليمات التنفيذية لقانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية** تجاوز حدود الدخول المشروع بالآتي: "*إن تجاوز حدود الدخول المشروع يعني تجاوز الصلاحيات الممنوحة للشخص المذكورة ضمن شروط الدخول لوسيلة تقانة المعلومات أو نظام المعلومات أو شبكة خاصة أو عامة*.

قد شدد المشرع عقوبة جريمة تجاوز حدود الدخول المشروع إذا قام الفاعل بعد تجاوز حدود الدخول المشروع بنسخ المعلومات التي وصل إليها، أو استخدمها، أو أفشاها، أو حذفها، أو بتعديلها. **ومن هنا نلاحظ التلاقي بين هذه الجريمة المنصوص عليها في المادة 11 من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية والجريمة المنصوص عليها في الفقرة ب من القانون رقم 12 لعام 2024.**

ثانياً: جريمة الدخول غير المشروع:

عاقب المشرع السوري على جريمة الدخول غير المشروع إلى نظام معلومات في **المادة الثانية عشرة من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية، حيث** يتمثل السلوك في جريمة الدخول غير المشروع إلى نظام معلومات أو موقع إلكتروني أو حساب شخصي **بفعل الدخول، وأن يكون دخولاً غير مشروع.**

* **الدخول:** يقصد بالدخول جميع الأفعال التي تسمح بالولوج إلى نظام معلومات أو موقع إلكتروني أو حساب شخصي والوصول إلى المعلومات المخزنة به. وفعل الدخول يمكن أن يتم بطريقة مباشرة أي بالدخول كمستخدم دون أن يكون للفاعل الحق أو التصريح للقيام بذلك، كما يمكن أن يتم الدخول بطريقة غير مباشرة أي عن بعد عن طريق الشبكات كالإنترنت، وغالباً ما يتم الدخول بالطريقة المباشرة من قبل العاملين في الجهات المجني عليها، أما الطريقة غير المباشرة فيرتكبها أشخاص لا ينتمون إلى هذه الجهات. (قورة، 2004، ص 322).

وقد عرفت المادة 12 من التعليمات التنفيذية لقانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية الدخول غير المشروع بالآتي:

"*كل من يدخل اختراقاً جهازاً حاسوبياً أو منظومة معلوماتية أو موقع إلكترونياً أو حساباً شخصياً بدون تصريح أو موافقة مسبقة من صاحب المنظومة وبأي طريقة كانت سواء عن طريق الشبكة أو احتيالاً*".

ولا شك أن مجرد الدخول إلى نظام معلومات أو موقع إلكتروني أو حساب شخصي لا يشكل بحد ذاته جريمة، وإنما يستمد هذا الدخول عدم مشروعيته من كونه دون وجه حق أو دون صلاحية أو غير مصرح به. (**الخن**، 2010، ص 114)

***عدم مشروعية الدخول:** يقصد بعدم مشروعية الدخول انعدام سلطة الجاني في الدخول إلى نظام معلومات أو موقع إلكتروني أو حساب شخصي، أي إذا كان دخول الفاعل قد تمّ من دون الحصول على تصريح من الشخص المسؤول عن النظام (**قورة،** *2004*، ص 333) وقد شدد المشرع عقوبة جريمة الدخول غير المشروع إذا قام الفاعل بعد الدخول بنسخ المعلومات التي وصل إليها، أو استخدمها، أو أفشاها، أو حذفها، أو بتعديلها. **ومن هنا نلاحظ التلاقي بين هذه الجريمة المنصوص عليها في المادة 12 من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية والجريمة المنصوص عليها في الفقرة ب من القانون رقم 12 لعام 2024 .**

ثالثاً : جريمة انتهاك الخصوصية:

نصت المادة 20 من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية على هذه الجريمة، حيث يتمثل محلها بالبيانات الشخصية السرية للفرد، وقد عرف المشرع السوري في المادة الأولى من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية الخصوصية بأنها: (*حق الفرد في حماية أسراره، الشخصية، أو الملاصقة للشخصية، أو العائلية، أو مراسلاته، أو سمعته أو نشاطاته على الشبكة*). فالخصوصية ترتبط بالشخصية الإنسانية، وهي عبارة عن مجموعة من الوقائع والعلاقات التي تسهم في تحديد هذه الشخصية، وتضم كافة العلاقات ذات الطابع الشخصي للإنسان، مثل الحياة العاطفية، والحالة الصحية، والحالة المدنية، ومحل الإقامة، والاتجاه السياسي. وقد نص المشرع في المادة 20 على أن النشاط الجرمي لهذه الجريمة يتمثل **بفعل النشر على الشبكة للمعلومات التي تتعلق بالخصوصية**، ويشترط أن يكون النشر دون رضاء صاحب هذه المعلومات. **ومن هنا نلاحظ التطابق بين هذه الجريمة المنصوص عليها في المادة 20 من قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية والجريمة المنصوص عليها في الفقرة ب من القانون رقم 12 لعام 2024 .**

الفرع الثالث:

حماية البيانات الشخصية وفقاً للقانون رقم 13 لعام 2021:

تضمن قانون الأحوال المدنية رقم 13 لعام 2021 مجموعة من النصوص القانونية التي حمت البيانات الشخصية سواء أكان الجاني من العاملين في الدولة أو من الغير.

أولاً: تجاوز حدود الدخول المشروع :

صدر **قانون الأحوال المدنية الجديد بالقانون رقم 13 لعام 2021** مكرساً مبدأً جديداً في تكريس "**أمانة سورية الواحدة**" والتي عرفها هذا القانون بأنها قاعدة البيانات التي تحوي جميع بيانات مواطني الدولة، وتُسجل فيها واقعاتهم أينما حدثت، ويتمثل فيها المواطن بقيد وحيد يُعرف برقمه الوطني.

نصت **الفقرة ج من المادة 72 من قانون الأحوال المدنية** على جريمة تجاوز حدود الدخول المشروع إلى منظومة السجل المدني المؤتمت، حيث اشترط المشرع أن يكون مقترف هذه الجريمة عاملاً مخولاً له الدخول إلى نظام السجل المدني المؤتمت. وبالتالي لا يمكن أن يقترف هذه الجريمة عامل غير مخول أو أن يقترفها شخص غير عامل . وتقترف هذه الجريمة بتجاوز صلاحيات الدخول المشروع، فيتوجب على العامل أن يتقيد بالتعليمات والصلاحيات الممنوحة له وفقاً للقانون، وبالتالي إذا دخل بشكل مشروع إلى منظمة معلوماتية تتعلق بالسجل المدني، وبدأ بالعمل عليها بشكل مخالف للتعليمات الخاصة بصلاحيات عمله على هذه المنظومة المعلوماتية فيعدُّ متجاوزاً لحدود الدخول المشروع. (**المخول،** *الجريمة الإلكترونية*، 2024 ، ص 294).

ثانياً : جريمة الدخول غير المشروع :

تنص الفقرة د من المادة 72 من قانون الأحوال المدنية على هذه الجريمة ، حيث تقترف بالدخول غير المشروع إلى منظومة معلوماتية للسجل المدني المؤتمت والوصول إلى المعلومات أو البرامج المخزنة عليها، وقد اشترط المشرع أن يتم الدخول من شخص ليس له الصلاحية للوصول لهذه المعلومات أو البرامج الإلكترونية. ويتوجب أن يتوافر لدى الجاني دافع محدد وهو أن تكون العلة التي حملت الجاني على ارتكاب الجريمة هي تعديل هذه المعلومات أو البرامج بالحذف أو الإضافة أو التعديل. **(المخول**، 2024، ص 296) **ومن هنا نلاحظ التلاقي بين هذه الجريمة المنصوص عليها في الفقرة د من المادة 72 من قانون الأحوال المدنية والجريمة المنصوص عليها في الفقرة ب من القانون رقم 12 لعام 2024** .

المطلب الثاني:

تفريد القواعد العقابية الناظمة لحماية البيانات الشخصية:

نص القانون رقم 12 لعام 2024 على مجموعة من الغرامات ذات الطابع المدني والتي تفرض بقرار من هيئة حماية البيانات الشخصية على بعض المخالفات المرتكبة من قبل المعالج أو المتحكم بالبيانات الشخصية إضافة لذلك نص على مجموعة من العقوبات السالبة للحرية والمالية والنفسية، كما نص على حالات تشدد العقوبة، ولذلك سنحلل في هذا المطلب أنواع عقوبات الجرائم المتعلقة بالبيانات الشخصية في الفرع الأول، وخصائص المعاقبة في الفرع الثاني.

الفرع الأول:

أنواع العقوبات للجرائم المتعلقة بالبيانات الشخصية:

تنوعت العقوبات المنصوص عليها في القانون رقم 12 لعام 2024 بين عقوبات جنائية وعقوبات جنحية وبين عقوبات سالبة للحرية وعقوبات مالية وعقوبات نفسية، وسنوضح السياسة العقابية للمشرع السوري من خلال إبراز هذا التنوع في العقوبات.

أولاً: تأمين الحماية بين العقوبات الجنائية والعقوبات الجنحية:

نص المشرع في القانون رقم 12 لعام 2024 على مجموعة من العقوبات الجنائية والجنحية، وتتسم السياسة العقابية للمشرع في هذا القانون بأنه جمع بين العقوبات السالبة للحرية والعقوبات المالية في النص التجريمي ذاته، ولم يترك تقديراً للمحكمة للاختيار بينهما، وذلك على عكس السياسة العقابية التي اعتمدها المشرع في العديد من النصوص ضمن قانون العقوبات أو في بعض التشريعات الجزائية الخاصة التي منحت الحق للمحكمة في تقدير أي من العقوبتين من الأفضل الحكم بها، وهذه السياسة الجديدة للمشرع السوري نجدها في العديد من التشريعات الخاصة الحديثة، ومن ذلك قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم 20 لعام 2022، وقانون حماية المستهلك رقم 8 لعام 2021 ، وبذلك تتضح معالم سياسة عقابية متشددة للمشرع السوري في الآونة الأخيرة .

إلا أنه لابد من الإشارة إلى أن **تعدد أسس القواعد التجريمية الناظمة لحماية البيانات الشخصية كما ذكرنا سابقاً أدى إلى تعدد العقوبات التي نص عليها المشرع للجرائم التي تقع على البيانات الشخصية في العديد من النصوص التشريعية** حيث نجد أن العقوبات التي نص عليها المشرع في القانون رقم 12 لعام 2024 تختلف عن العقوبات التي نص عليها المشرع في القانون رقم 20 لعام 2022 أو القانون رقم 13 لعام 2021 على الرغم من أن محل الجريمة هو نفسه وهو البيانات الشخصية المعالجة إلكترونياً، كما أن المصلحة المحمية هي ذاتها. إن هذا التعدد يقود إلى حالة من التضخم التشريعي غير المرغوب بها.

إن القانون علم إنساني يقوم على فكرة الغاية، كما هو حال علم الأخلاق وعلم الجمال وعلم المنطق، فهي علوم إنسانية لأنها تجعل من تفكير الإنسان السليم وتنمية تذوقه للجمال وضبط سلوكه وحمايته غاية لها، وهي علوم غائية معيارية لأن لكل علم منها غايته التي يسعى إلى إدراكها وفقاً لمعيار محدد، فغاية علم المنطق التفكير السليم، ومعياره الحق والصواب، وغاية علم الجمال تربية الشعور على تذوق الجمال وتمثله، ومعياره الذوق السليم، وغاية علم الأخلاق ضبط سلوك الإنسان ومعياره العدالة والخير والفضيلة، وغاية قانون حماية البيانات الشخصية هي حماية خصوصية الأفراد، وربط ذلك بأمن واستقرار ومصلحة الجماعة، ومعياره وضوح السياسة العقابية للمشرع السوري في حماية هذه الخصوصية.

لذلك فإن توحيد النصوص التشريعية التي تحمي هذه البيانات هو الغاية التي يتوجب على المشرع السوري تحقيقها بغرض توحيد العقوبات التي تستهدف النماذج القانونية نفسها المنصوص عليها في أكثر من قانون.

ثانياً: العقوبات النفسية:

وهي التي تمس المحكوم عليه في سمعته وقدره، فتنقص من احترامه بين الناس وتشهر به. **وقد جاءت أحكام هذه العقوبة في المادة 68 من قانون العقوبات،** وهي عقوبة إضافية جوازية، سواء قضى الحكم بعقوبة جنائية أو جنحية، ولكن في الحالة الأخيرة، أي إذا كان الحكم صادراً بعقوبة جنحية، فلا يجوز نشره إلا إذا كانت الجريمة من الجنح التي يجيز فيها القانون ذلك بنص خاص **(السراج** ، *شرح قانون العقوبات العام*، 2014، ص 378). ولا يجوز أن ينشر من الحكم إلا خلاصته، ما لم يرد نص استثنائي يقضي بنشر الحكم برمته. ويكون النشر في جريدة أو جريدتين يعينهما القاضي، غير أنه إذا كانت الجناية أو الجنحة قد اقترفت بواسطة جريدة أو أية نشرة دورية أخرى، جاز للقاضي أن يأمر بنشر إعلان إضافي فيها. ويلزم المحكوم عليه بنفقات نشر الحكم. ولضمان تنفيذ عقوبة نشر الحكم فرض المشرع غرامة تبدأ من مئة ألف ليرة وقد تصل إلى خمسمئة ألف ليرة على المدير المسؤول للصحيفة التي اختيرت لنشر الإعلان، إذا رفض أو أرجأ نشره.

نص القانون رقم 12 لعام 2024 على هذه العقوبة النفسية وهي نشر الحكم في المادة 39 منه: " تقضي المحكمة بنشر حكم الإدانة في صحيفتين محليتين، وعلى موقع الهيئة الإلكتروني على نفقة المحكوم عليه".

ومن خلال المقارنة بين نصي **المادتين68 من قانون العقوبات و 39 من القانون رقم 12 لعام 2024** نجد أن المشرع السوري خرج عن القواعد العامة لعقوبة نشر الحكم حيث أن هذه العقوبة جوازية يعود تقدير فرضها للمحكمة إلا أن القانون رقم 12 لعام 2024 جعلها وجوبية . مما يؤكد السياسة العقابية المتشددة للمشرع السوري في هذا القانون حرصاً منه على تأمين الحماية الجزائية اللازمة للبيانات الشخصية.

الفرع الثاني:

خصائص المعاقبة:

نتابع في هذا الفرع دراسة السياسة العقابية التي اتبعها المشرع السوري في القانون رقم 12 لعام 2024 من خلال دراسة خصائص المعاقبة سواء من حيث الظروف التي تشدد العقوبة، أو الشروع في الجريمة، أو الغرامات ذات الطابع المدني.

أولاً: تشديد العقوبة:

تعدُّ العقوبات المنصوص عليها في القانون رقم 12 لعام 2024 عقوبات شديدة سواء لجهة العقوبات السالبة للحرية الجنائية أو الغرامات ولذلك لم ينص المشرع في هذا القانون على حالات لتشديد هذه العقوبات، إلا في حالة وحيدة فقط عندما شدد عقوبة الجريمة المنصوص عليها في الفقرة ب من المادة 37 وهي جريمة جمع أو عالج أو أفشى أو أتاح أو تداول أو خزن أو نقل أو حفظ أو حذف بيانات شخصية معالجة إلكترونياً بأي وسيلة من الوسائل دون موافقة صاحب البيانات أو في غير الأحوال المصرح بها قانوناً، حيث شدد عقوبة هذه الجريمة إلى الحبس من ستة أشهر إلى سنتين وبغرامة من سبعة ملايين إلى عشرة ملايين ليرة سورية في إحدى الحالات الآتية:

1 . إذا ارتكب الجرم بقصد جلب منفعة مادية أو معنوية، أو بقصد تعريض صاحب البيانات للخطر أو الضرر.

2. إذا كانت البيانات شخصية حساسة.

وبذلك فإن تشديد عقوبة هذه الجريمة يرتبط من جهة بالدافع الذي قاد الجاني إلى ارتكاب الجريمة حيث أنه يتوجب لتشديد العقوبة أن تكون العلة التي حملت الجاني إلى اقتراف جريمته هي جلب منفعة مادية أو معنوية أو تعريض صاحب البيانات للخطر أو الضرر وبالتالي فهنا ظرف التشديد يرتبط بالجاني نفسه فهو ظرف تشديد شخصي يطال المسهم في الجريمة في حال توافر عنده الدافع ذاته، **وذلك سنداً للفقرة الثالثة من المادة 215 من قانون العقوبات :** "*وأما ما سوى ذلك من الظروف فلا يتناول مفعولها إلا الشخص الذي تتوافر فيه*".

أما ظرف التشديد الثاني فيتعلق بمحل الجريمة حيث يجب أن يكون هذا المحل بيانات شخصية حساسة ويقصد بها البيانات التي تفصح عن الصحة النفسية أو العقلية أو البدينة أو الجينية أو بيانات القياسات الحيوية البيومترية أو البيانات المالية أو المعتقدات الدينية أو الآراء السياسية أو الحالة الجنائية أو بيانات الأطفال وفاقدي الأهلية ، بالتالي فهنا ظرف التشديد يرتبط بالجريمة نفسها فهو ظرف تشديد مادي يطال كل الشركاء أو المتدخلين في الجريمة سنداً **للفقرة الأولى من المادة 215 من قانون العقوبات:** " مفاعيل الأسباب المادية التي من شأنها تشدد العقوبة تسري على كل الشركاء في الجريمة والمتدخلين فيها ".

ثانياً: الشروع:

تابع المشرع سياسته العقابية المتشددة من خلال عقابه على اقتراف الشروع في الجنح المنصوص عليها في القانون رقم 12 لعام 2024 ، **حيث نصت المادة 38** على الآتي: "*يعاقب على الشروع في الجنح المنصوص عليها في هذا القانون وفقا الأحكام الواردة في قانون العقوبات*". وبذلك عاقب المشرع على الجنح بغض النظر عن طبيعة الجنحة، وهذا لا ينسجم مع طبيعة بعض الجرائم المنصوص عليها في القانون رقم 12 لعام 2024 حيث أن بعض هذه الجرائم جرائم يتمثل ركنها المادي بالامتناع عن القيام بفعل فهي جرائم سلبية لا يمكن تصور الشروع فيها أساساً **(بهنام**، 1995، ص 583)، فكيف يمكن أن نعاقب على الشروع في اقترافها **ومن ذلك الجريمة المنصوص عليها في الفقرة هـ من المادة 37.**

ولابد من الإشارة إلى أن القانون رقم 12 لعام 2024 طبق القواعد العامة للشروع المنصوص عليها في قانون العقوبات على الجرائم المنصوص عليها في القانون رقم 12 لعام 2024 وبذلك منح للمحكمة السلطة التقديرية في تخفيف العقوبة في حال كان الجرم مشروعاً فيه شروعا تاماً أم ناقصاً **(السراج**، *شرح قانون العقوبات العام*، 2014، ص 245)، ولم ينص على القاعدة الاستثنائية التي طبقها في بعض التشريعات الجزائية الخاصة من حيث المساواة بين عقوبة الجريمة التامة والجريمة المشروع فيها كما هو

الحال مثلا في قانون العقوبات الاقتصادية (**السراج**، *شرح قانون العقوبات الاقتصادي في التشريع السوري والمقارن*، 2011، ص 230) أو في قانون المخدرات (**المخول**، *قانون المخدرات*، 2011، ص 90)، وبذلك خفف المشرع من وطأة السياسة العقابية المشددة التي اتبعها في باقي أحكام القانون رقم 12 لعام 2024.

ثالثاً : الغرامات ذات الطابع المدني :

منح المشرع السوري في بعض القوانين الجهات العامة فرض نوع من الغرامات ذات الطابع المدني ومن ذلك مثلاً قانون الاتصالات رقم 18 لعام 2010 الذي منح الهيئة الناظمة للاتصالات والبريد سلطة فرض غرامات على المخالفين لبعض أحكام قانون الاتصالات، وهذا ما كرره المشرع في المادة 36 من القانون رقم 12 لعام 2024 حيث منح هيئة حماية البيانات الشخصية سلطة فرض غرامات مالية تدرج من مليون إلى خمسة عشر مليون ليرة سورية كل من يخالف بعض الواجبات المنصوص عليها في هذا القانون ومثال ذلك يعاقب المتحكم أو المعالج بالغرامة مليون ليرة سورية إذا امتنع عن تمكين صاحب البيانات من ممارسة حقوقه المنصوص عليها في المادة الثالثة من القانون ومن ذلك الامتناع عن إبلاغه بأي خرق لبياناته الشخصية، كما عاقب بالغرامة عشرة ملايين ليرة سورية كل مسؤول حماية البيانات الشخصية لم يلتزم بأحد واجباته المنصوص عليها في المادة العاشرة من القانون ومن ذلك عدم قيامه بالتقييم والفحص الدوري لنظم حماية البيانات الشخصية. كما عاقب بالغرامة خمسة عشر مليون ليرة سورية كل معالج لم يلتزم بواجباته المنصوص عليها في المادة السادسة ومن ذلك عدم محو البيانات الشخصية بانقضاء مدة معالجة البيانات الشخصية.

ولابد من الإشارة إلى أن **الفقرة د من المادة 36 من القانون رقم 12 لعام 2024** تضمنت نصاً غير دقيق من حيث صياغته التشريعية: "*تفرض بقرار من الهيئة غرامة مالية ثلاثة ملايين ليرة سورية (كل ممثل قانوني للشخص الاعتباري) لم يلتزم بما نصت عليه المادة التاسعة*".

وبالعودة لنص **المادة التاسعة من القانون رقم 12 لعام 2024 نلاحظ أن الفقرة الأولى** منها نصت على الآتي : "*في حال كان المتحكم أو المعالج شخصاً اعتبارياً ،يلتزم بتعيين عامل مختص مسؤول عن حماية البيانات الشخصية، ويتم قيده في سجل مسؤولي حماية البيانات الشخصية في الهيئة، ويعلن عن ذلك على موقع الهيئة الإلكتروني* ".

وبالتالي فإن الالتزام الواجب على كل متحكم أو معالج في حال كان شخصاً اعتبارياً هو تعيين عامل مسؤول عن حماية البيانات الشخصية فإذا لم يقم بذلك فيعدُّ غير ملزم بما نصت عليه المادة التاسعة، وتفرض عليه الغرامة المنصوص عليها في **الفقرة د من المادة 36 من القانون رقم 12 لعام 2024**، لكن عند قراءة نص هذه الفقرة يتبين أن الغرامة تفرض على الممثل القانوني للشخص الاعتباري وليس على الشخص الاعتباري نفسه وهذا يخالف المبدأ القانوني العام بالفصل بين الذمة المالية للشخص الاعتباري والذمة المالية لممثله القانوني (B.BOULOC, 2021 , p. 234)، وهنا المسؤولية تقع على الشخص الاعتباري لأنه لم يقم بتعيين مسؤول عن حماية البيانات الشخصية ولا يمكن أن تقع على ممثل الشخص الاعتباري كون الذمة المالية للشخص الاعتباري منفصلة عن الذمة المالية للشخص الطبيعي أي الممثل القانوني فعدم الالتزام قد اقترفه الشخص الاعتباري عن طريق ممثله القانوني.

الخاتمة:

تزايدت البيانات الشخصية تزايداً كبيراً لدرجة بات معها أمر حفظها يستلزم مكتبات كبيرة وأماكن واسعة، كما أن تصنيفها وتبويبها يتطلبان وقتاً وجهداً كبيرين، والرجوع إليها لا يقل عن ذلك جهداً ووقتاً، فكان لابد من التفكير بوسيلة يتم من خلالها تجاوز هذه المشكلة، فظهرت وسائل تقانة المعلومات لتستوعب هذا الكم الكبير من البيانات فتم تخزينها ومعالجتها فصارت البيانات قابلة للتداول بسرعة كبيرة. هذه الميزات الكبيرة لوسائل تقانة المعلومات جعلت الاستعانة بها ضرورة لا غنى عنها لدى كافة الجهات العامة والجهات الخاصة التي تتحكم وتعالج البيانات الشخصية، إلا أن هذه الوسائل قد تكون عرضة للاختراق، كما أن القائمين ضمن هذه الجهات قد يتعسفون في استعمال حقهم بالاطلاع على هذه البيانات، مما دفع المشرعين في دول العالم لإصدار القوانين لحماية هذه البيانات الشخصية ومنهم المشرع السوري.

وبعد تحليل القانون رقم 12 لعام 2024 وفقاً للدراسة أعلاه، تمكنا من الوصول إلى **النتائج الآتية:**

1 . عرف قانون حماية البيانات الشخصية هذه البيانات بشكل واضح سواء أكانت هذه البيانات عادية أو حساسة كونها تشكل محلاً للجرائم المتعلقة بهذه البيانات، وذلك احتراماً لمبدأ الشرعية.

2. حدد قانون حماية البيانات الشخصية حقوق أصحاب البيانات الشخصية وشروط جمع ومعالجة البيانات والمعايير والضوابط اللازمة لجمع ومعالجة البيانات الشخصية والتزامات الجهات القائمة على هذه المعالجة من خلال النص على التزامات واضحة تجاه المتحكم والمعالج.

3. نص قانون حماية البيانات الشخصية على ضرورة توافر مسؤول لحماية البيانات الشخصية، مع تحديد الالتزامات الواقعة عليه.

4. نص قانون حماية البيانات الشخصية على غرامات ذات طابع مدني يمكن لهيئة حماية البيانات فرضها على المخالفين لبعض أحكامه.

5. قسم المشرع الجرائم المنصوص عليها في هذا القانون إلى قسمين القسم الأول يرتكب من قبل المعالج أو المتحكم والقسم الثاني يرتكب من أي شخص.

6 . لم ينص المشرع السوري على حماية البيانات المعالجة إلكترونياً للشخص الاعتباري، حيث قصر نطاق الحماية على البيانات الشخصية للشخص الطبيعي.

انطلاقاً من هذه النتائج، وما توصلنا إليه من تحليل للقانون رقم 12 لعام 2024، **يمكن أن نخلص إلى مجموعة من المقترحات :**

1 . الابتعاد عن النصوص القانونية الجزائية المتعددة التي حمت البيانات الشخصية سوءاً في قانون حماية البيانات الشخصية رقم 12 لعام 2024 أو قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية رقم 20 لعام 2022 أو قانون الأحوال المدنية رقم 13 لعام 2021 وجعل الحماية القانونية الجزائية لهذه البيانات من خلال نموذج قانوني موحد، وذلك تلافياً للتناقض بين أركان هذه الجرائم والعقوبات في النماذج القانونية المختلفة .

2. إضافة ظروف تشديد تتعلق بشخص المجنى عليه كأن تكون البيانات تتعلق بأشخاص من ذوي الاحتياجات الخاصة أو عند تعدد المجني عليهم.

3. التمييز في العقوبة في حال إذا كان البيانات عادية أو بيانات حساسة، حيث أن المشرع لم يفرق في حمايتها الجزائية عند وقوع إحدى الجريمتين المنصوص عليهما في الفقرتين د و هـ من المادة 37 من القانون رقم 12 لعام 2024 . حيث ينبغي أن تكون عقوبة الاعتداء على البيانات الشخصية الحساسة أشد من عقوبة الاعتداء على البيانات الشخصية العادية، وذلك كون الضرر الذي يقع على الشخص المعني بهذه البيانات سيكون أشد جسامة.

4. لم ينص المشرع على جرائم غير مقصودة في هذا القانون على الرغم من أن تشديد الحماية الجزائية يستتبع أن يكون للركن المعنوي لبعضها صورة غير مقصودة . ولذلك نقترح أن يجد الإهمال أو قلة الاحتراز الطريق لتكوين نموذج قانوني لحماية البيانات الشخصية من خلال تمثيل الركن المعنوي بالخطأ الواعي أو الخطأ غير الواعي، وخاصة في الجرائم المقترفة من قبل المعالج أو المتحكم، ومنها الجرائم المنصوص عليها في الفقرتين أ، هـ من المادة 37 من القانون رقم 12 لعام 2024.

5 . منح الأعذار المحلة والأعذار المحلة للمسهم في الجريمة المنصوص عليها في الفقرة ب من المادة 37 من القانون رقم 12 لعام 2024 باستثناء المحرض في بعض الحالات التي تسمح بالكشف عن باقي المسهمين في الجريمة كون جريمة الاعتداء على البيانات الشخصية قد لا تترك أدلة على اقترافها مما يجعل أمر الكشف عن مقترفيها أمراً صعباً .

6 . توسيع محل جريمة الاعتداء على البيانات الشخصية المعالجة إلكترونياً ليشمل الأشخاص الاعتباريين وفقاً للشروط التي ذكرناها في دراستنا، وليشمل البيانات الشخصية المنشورة على الشبكة للمواطنين الأجانب في حال تمت معالجة بياناتهم من قبل متحكمين أو معالجين يخضعون لأحكام القانون رقم 12 لعام 2024.

7 . يتوجب على المشرع التفريق في التجريم والعقاب بين المعالجة غير المشروعة للبيانات الشخصية وبين الإتاحة غير المشروعة لهذه البيانات، وفرض عقوبة أشد على المعالجة غير المشروعة، وذلك لما تسببه من ضرر جسيم على الشخص صاحب البيانات الشخصية.

وأخيراً يمكن القول إن مسألة وضع قواعد ثابتة وتطبيقها على أشياء قابلة للتطور بشكل سريع ليس أمراً سهلاً، وخاصة إذا كانت هذه الأشياء تتعلق بالبيانات الشخصية المعالجة إلكترونياً وذلك لأن القواعد التي توضع لضمان المحافظة على البيانات يصعب تطبيقها في فترة لاحقة بسبب تطور وسائل تقانة المعلومات، وهذا الأمر يجعل المشرع السوري في تحدي دائم لتعديل القوانين الناظمة لحماية هذه البيانات.

التمويل:

هذا البحث ممول من جامعة دمشق وفق رقم التمويل (501100020595).

المراجع:

1. **حسان** أ. ، نحو نظرية عامة لحماية الحياة الخاصة في العلاقة بين الدولة والأفراد، دار النهضة العربية، القاهرة ، مصر ، 2001
2. **القايد** أ. ، الحماية الجنائية للحياة الخاصة وبنوك المعلومات ، القاهرة ، مصر ، 1988
3. **بهنام** ر. ، النظرية العامة في القانون الجنائي ، منشأة المعارف ، القاهرة ، مصر ، 1995
4. **سلبي** ز. ، جريمة الابتزاز الإلكتروني ، دار الأكاديميون للنشر والتوزيع ، عمان ، الأردن ، 2021
5. **الخن** ط.، الجرائم المعلوماتية ، منشورات الجامعة الافتراضية السورية، دمشق ، 2010
6. **عباس** ع. ، حقوق الإنسان ، دار الفاضل ، دمشق ، سورية، الجزء الثالث ، 1995
7. **السراج** ع. ، شرح قانون العقوبات العام ، منشورات جامعة دمشق، دمشق ، 2014
8. **السراج** ع. ، شرح قانون العقوبات الاقتصادي في التشريع السوري والمقارن ، منشورات جامعة دمشق ، دمشق ، 2011
9. **المخول** ع. ، قانون المخدرات ، منشورات الجامعة الافتراضية السورية ، دمشق، 2011
10. **المخول** ع. ، الجريمة الإلكترونية ، دار القلم ، سورية ، دمشق ، 2024
11. **المقاطع** م. ، **1992** حماية الحياة الخاصة للأفراد وضماناتها في مواجهة الحاسوب الآلي ، مطبوعات جامعة الكويت، الكويت.
12. **الشهاوي** م. ، الحماية الجنائية لحرمة الحياة الخاصة ، دار النهضة العربية ، القاهرة ، مصر ، 2005
13. **سري طه** م. ، **الكمبيوتر في مجالات الحياة ، الهيئة المصرية العامة للكتاب ، القاهرة، مصر ، 1988**
14. **الرواشدة أ. ، جريمة الابتزاز الإلكتروني في القانون الأردني ، مركز الكتاب الأكاديمي ، عمان ، الأردن، 2022**
15. **العوجي م. ، المسؤولية الجنائية في المؤسسة الاقتصادية ، مؤسسة نوفل ، بيروت ، لبنان ، 1990**
16. **قورة ن.، جرائم الحاسب الآلي الاقتصادية ، منشورات الحلبي الحقوقية بيروت ، لبنان، 2004**
17. **مغبغب ن. ، مخاطر المعلوماتية والإنترنت ، منشورات الحلبي الحقوقية ، لبنان ، بيروت 1998**
18. **رستم هـ. ، قانون** العقوبات ومخاطر تقنية الحاسوب ، مكتبة الآلات الحديثة ، أسيوط، مصر، 1992
19. ANTONIO J., La protection de la vie privée face au développement d'informatique, Thèse, Paris, 1976,
20. BOULOC B., Droit pénal général, Dalloz, 2021
21. BUTZ J., Criminalité informatique, éd. Larcier, 2019
22. GARE T., Droit pénal et procédure pénale, éd. LexisNexis, 2022
23. LINODON R., Les droits de la personnalité, Dalloz, Paris, 1974 ,
24. PRADEL J., Droit pénal général, éd. Dalloz, 2005,
25. VITU R., Droit pénal spécial, éd. Cujas, 1981
26. ANDERSON R., Measuring the cost of cybercrime, University of Cambridge, 2012.

27. **السيد** أ.، الحماية الجنائية لحق الإنسان في حياته الخاصة، أطروحة دكتوراه في القانون، جامعة المنصورة، مصر، 1983.
28. علي ر.، الحماية الجنائية للمعلومات على شبكة الإنترنت، أطروحة دكتوراه في القانون، جامعة القاهرة، مصر، 2009
29. خليفة ش.، "شبكات المعلومات"، مجلة المكتبات والمعلومات العربية، دار المريخ للنشر، العدد الثاني، نيسان 1984، ص 12
30. الفيومي ع.، "جرائم الحاسب الآلي"، مجلة المحامون، دمشق، سورية، 2000، ص 1240
31. الفحل ع.، "جرائم الحاسب الآلي"، مجلة المحامون، دمشق، سورية ، 1995، ص 672