حِماية الخُصوصيّة

في

الرِّعاية الصِحيّة

البَيانات الطِّبية و التَّحديات القانونيِّة

قصي عصام قطشة

2023

بسم الله الرحمن الرحيم

وبعدَ الصَّلاة والسَّلامِ على سيدنا محمد خير المرسلين

إنَّ الحفاظَ على الخصوصيَّةِ وحمايةَ السّريَّةِ هما قيمتانِ أساسيتانِ في الدين الإسلامي ، إذ إنَّه يؤكّدُ على احترامِ حقوقِ الأفرادِ ويحثُّ على حفظِ خصوصيَّتهم في مختلفِ جوانبِ حياتهم ، و يؤكّدُ الإسلامُ أنَّ الإنسانَ يتمتَّعُ بحقوقٍ وكرامةٍ مطلقةٍ ، ومن هذه الحقوق حق الخصوصية ، وبالتالي فإنَّ الإسلامَ يحثّ على احترامِ خصوصيَّةِ الأفرادِ وعدم انتهاكها دونَ وجهٍ حق.

يعدُّ الإسلامُ الخصوصيةَ والسّريَّة جزءًا من حقوقِ الإنسانِ الأساسيَّةِ ، إذ يجبُ على المسلمينَ احترامُ خصوصيَّةِ الآخرينَ وعدمُ التجسُّسِ على حياتِهم الشخصيَّةِ أو إفشاءُ أسرارهم ، كما و يُعدُّ تجاوزُ حقوقِ الأفرادِ والتَّطفلُ على خصوصِيتهم أمراً مرفوضاً في الإسلام، إلا في حالاتِ الضرورةِ القُصوى ومصلحةِ المُجتمع .

أمَّا في العلاقاتِ الزوجيَّةِ ، فينصحُ الإسلامُ بالثّقةِ والصّدقِ واحترامِ خصوصيَّةِ شريكِ الحياة ، إذ يجبُ على الزوجينِ عدمُ الانتهاكِ المُتعمَّدِ لخصوصيَّةِ بعضهما بعضاً ، وعدمُ الكشفِ عن أسرارِ الحياةِ الزوجيَّةِ لأشخاصٍ آخرينَ ، كما تعدُّ الثّقةُ والحفاظُ على الخصوصيَّةِ أساساً في بناءِ علاقاتٍ زوجيةٍ قويَّةٍ ومستدامة .

أمَّا في المجتمعِ بشكلٍ عام ، يدعو الإسلام إلى احترامِ خصوصيَّةِ الأفرادِ وعدمِ التَّدخلِ في حياتهم الشَّخصيَّة دونَ وجهِ حق ، لذلكَ يجبُ علينا أنْ نحترمَ حقوقَ الآخرينَ وأنْ نعاملَ الأشخاصَ بعدلٍ وإنصافٍ ، دونَ تجسُّسٍ أو تشهيرٍ أو نشرِ شائعات.

إذاً يمكنُنا القولُ بأنَّ الإسلامَ يشجّعُ على حفظِ الخصوصيَّةِ والسّريَّةِ في مختلفِ جوانبِ الحياةِ ، إذ يعدُّ احترامَ خصوصيَّةِ الآخرينَ وعدمُ انتهاكِها أمراً مهمَّاً في تعاليمِ الإسلامِ، حيثُ يعكسُ قيمَ العدلِ والأمانةِ والرَّحمة الَّتي تميزُ الإسلام .

لذا قرَّرتُ ألَّا أوفّرَ جهداً يمكنُنِي بذلُهُ لشرحِ وتوضيحِ مبادئ حمايةِ البياناتِ الَّتي كانت ألمانيا دولةً سبَّاقةً لتشريعِ وسنّ قوانينَ تحمي خصوصيَّةَ الأفرادِ وتعاقبُ من يتجاوزها.

و في هذا الكتابِ سأُلقي الضوءَ على التشريعاتِ واللوائحِ المتعلّقةِ بحمايةِ البياناتِ ، وكيفيَّةِ الامتثالِ لها وتطبيقِها في بيئاتٍ مختلفةٍ في القطاعِ الصّحي، كما سألقي الضوءَ على مفهومِ الخصوصيَّةِ وحقوقِ المُستخدمينَ والأسسِ القانونيَّةِ المُتعلّقةِ بجمعِ واستخدامِ البياناتِ الشَّخصيَّةِ و الطبية.

و أعتذرُ مسبقاً في حالِ وجودِ كلماتٍ غيرِ واضحةٍ وذلكَ بسببِ عدمِ توفُّرِ ترجمةٍ لجميعِ المصطلحاتِ المستخدمةِ في هذهِ التشريعات .

أنسِبُ الفضلَ لله تعالى الَّذي مكنَّني من إنجازِ هذا العملِ و إنّ كانَ صحيحاً فهو من عند الله وبتوفيقه لي وإنْ وُجِدَ خطأ فهو منّي .

ختاماً أُهدي هذا العملَ لوالديَّ اللّذانِ علَّماني الإخلاصَ بعملي و فعلَ كلّ ما يسعُني لتقديمِ علمِيَ لمَنْ يحتاجه ، و أؤكّدُ أنَّ هذا الكتابَ مجانيٌّ بالكاملِ ولا يجوزُ لأيّ شخصٍ نسبُ هذا العملِ كاملاً أو جزءً منهُ لنفسهِ أو فرضِ رسومٍ لمشاركةِ الكتابِ أو تحميلهِ تحتَ طائِلةِ الملاحقةِ القانونيَّةِ والقضائيَّةِ .

والله ولي التوفيق

قصي عصام قطشه

الاختصارات الَّتي استُخدِمَت في الكتاب

BDSG قانون حماية البيانات الألماني .

DSGVO – GDPR اللوائح الأوروبية العامة لحماية البيانات .

DPC - لجنة حماية البيانات الإيرلندية .

StGB - قانون العقوبات الألماني .

MBO-Ä المرجعية النموذجية لقوانين مزاولة مهنة الطبيب .

SGB - قانون الضمان الاجتماعي .

BGB – القانون المدني الألماني .

UWG- قانون مكافحة المنافسة غير العادلة .

(PatientenRG (Patientenrechtegesetz) - قانون حقوق المرضى .

(GG (Grundgesetz – القانون الألماني الأساسي .

BÄO قانون الأطباء الفيدرالي .

MPG- قانون المنتجات الطبية .

الفهرس

أهمية حماية البيانات في ألمانيا

تنبعُ أهميَّةُ حمايةِ البياناتِ في ألمانيا من اعتبارِها جزءاً لا ينفكُّ من حُرمةِ الكرامةِ الإنسانيَّة و الحقّ في حريَّةِ التَّصرّفِ ، و اللذَّان ذُكِرا في القانونِ الأساسيّ للجمهوريَّةِ الاتّحاديَّةِ الألمانيَّةِ الّذي أقرّهُ المشرّعُ في المحكمةِ الدّستوريَّةِ الألمانيَّةِ .

و قد ذُكِرَ في المادةِ الأُولى للفصلِ الأوَّل في القانونِ الأساسيّ الألمانيّ :

ـ لا يجوزُ المَساسُ بكرامةِ الإنسانِ ، لأنَّ باحترامِها و صونِها تلتزمُ جميعُ السُّلطاتِ في الدَّولة .

أمَّا في المادَّةِ الثانية بفصليها الأوَّلِ و الثَّاني اللذان أعتبرهما في المقامِ الأول فقد أُخذا بعينِ الاعتبارِ عندَ إقرارِ التَّشريعاتِ الخاصَّةِ بحماية البيانات ، حيث ذكر المشرّعُ في المادة ما يلي :

1- كلُّ فردٍ لهُ الحقُّ في التعبيرِ عن شخصيَّتِهِ ، طوالَ عدمِ انتهاكِهِ حقوقَ الآخرين ، و عدمِ إخلالِهِ بالنّظام .
2- كلُّ فردٍ لهُ الحقُّ في الحياةِ و في السَّلامةِ الشخصيَّةِ ، ولا يجوز انتهاكُ حريّةِ الفردِ ، و لا يُسمَحُ بالتَّدخلِ بهذه الحقوق إلاَّ بموجبِ قانونٍ ينصُّ على ذلك ، و هنا انبثقَ المصطلحُ الأكثرُ خصوصيَّةً في حمايةِ البياناتِ ، و هو حقُّ تقرير المصيرِ المعلوماتي .

و يشيرُ المصطلحُ إلى حقّ الأفرادِ بالتحكّمِ بالبياناتِ المتعلّقةِ بهم ، و الَّتي تمَّ جمعُها و معالجتُها من قِبَلِ الشَّركاتِ ، أو المؤسَّساتِ ، أو الحكوماتِ .

و يشملُ هذا الحقُّ معرفةَ ما إذا كانت البياناتُ الشَّخصيَّةُ قيدَ الاستخدامِ ، و ما الغرضُ من استخدامها ، و الحقّ بالوصولِ إليها ، و الحقّ في تحديدِ إمكانيَّةِ مشاركةِ البياناتِ مع طرفٍ ثالث .

و يشملُ المفهومُ الحقَّ في حذفِ البياناتِ الشخصيَّةِ إذا لم يعدْ هناكَ غرضٌ لجمعها و معالجتِها ، أو إذا تمَّ جمعُها و معالجتُها بصورةٍ قانونيَّة .

يتمُّ الحفاظُ على هذا الحقّ و حمايته عبرَ القوانينِ و اللوائحِ الَّتي تحمي خصوصيَّةَ الأفرادِ و تحدُّ من جمعِ و استخدامِ البياناتِ الشخصيَّةِ بدونِ إذن .

و في عصرِ الرقمنةِ كانَ من الضروريّ تعديلُ و إضافةُ لوائحَ إضافيَّةَ لحمايةِ الأفرادِ في المقامِ الأوَّلِ ، و من ثمَّ حمايةِ بياناتهم الشخصيَّةِ.

لذلكَ تمَّ إقرارٌ من المحكمةِ الدستوريَّةِ الألمانيَّةِ عامَ 2008 ينصُّ على الحقّ في الخصوصيَّةِ الرقميَّةِ ، و هو حقٌّ للأفرادِ في الحفاظِ على خصوصيَّتهم و حمايةِ البياناتِ الشخصيَّةِ الَّتي تمَّ جمعها و معالجتها عبر الإنترنت ، و الحقّ في الموافقةِ على جمعِ و معالجةِ هذه البيانات .

و يشملُ هذا المفهومُ الحقَّ في الحفاظِ على الخصوصيَّةِ الرقميَّةِ ، و الحقَّ بالتحكُّمِ في معلوماتِ الاتّصالِ الخاصَّةِ بالأفرادِ مثل البريدِ الإلكتروني و الهاتفِ و الرسائلَ النَّصيَّةِ و الحقَّ بحمايةِ بياناتِ التصفّح و التسوّقِ عبر الإنترنت ، و الحقَّ في عدمِ الكشفِ عن هويَّةِ الأفراد على الإنترنت إلَّا بموافقتهم الصَّريحة .

يتمُّ تطبيقُ هذا المفهومِ في العديدِ من الدول ، و قد تمَّ تطويرهُ لتوفيرِ إطارٍ قانوني يحمي خصوصيَّة الأفرادِ ، و يحدُّ من جمعِ و معالجةِ البياناتِ الشخصيَّةِ بدون إذن.

و الجديرُ بالذكرِ أنَّ أولَ قانونٍ في العالم لحمايةِ البياناتِ بشكلهِ الحاليّ كان القانونَ الخاصَّ بمقاطعة (هيسن Hessen) ، و تمَّ إقرارهُ في عامِ 1970 ، لهذا تُعدُّ ألمانيا دولةً رائدةً عالميَّاً في مجالِ حمايةِ البياناتِ ، و هذا لحمايةِ جميعِ الحقوقِ المذكورةِ أعلاه ، و التَّي ضمنها الدستورُ الألمانيُّ لأفرادِ المجتمع .

و لعلَّ كلمةَ أحدِ المعلّمين الجامعيّين لي خلالَ إحدى المحاضراتِ تلخّصُ كثيراً من الكلامِ عندما قال لي :

" في ألمانيا ، نحنُ نصدرُ قوانينَ و نعدُّ لها حسب الحاجةِ لحمايةِ الأفرادِ و ليسَ لحمايةِ أرقامٍ و أحرفٍ مخزَّنةٍ على أجهزةِ الحاسب " .

بدايةً من الضروريّ فهمُ المصطلحاتِ الّتي تُستَخدمُ لأنَّها مصطلحاتٌ قانونيَّةٌ ، قد لا تُفهَمُ من المرَّةِ الأولى الّتي تُسمَعُ بها ، و لتجنّبِ سوءِ فهمِ هذه المُصطلحاتِ ، فقد عرَّفَ المشرّع في المادةِ الرابعةِ من قانونِ DSGVO.

البياناتُ الشَّخصيَّة : و تعني البياناتِ الَّتي تتعلَّقُ بشخصٍ محدَّد أو يمكنُ تحديدُه ، مثلَ الاسمِ و العنوانِ و رقمِ الهاتفِ و البريدِ الإلكترونيّ و التفاصيلِ الماليَّةِ و المواقعِ الجغرافيَّةِ و الصورِ و الفيديوهاتِ ، و أيّ معلوماتٍ أُخرى يمكنُ استخدامُها للتعرّفِ على شخصٍ ما .

مثال : يوجدُ في غرفةٍ خمسةُ أشخاصٍ واحدٌ فقط من أصلٍ غيرِ ألماني ، و هذا معلومٌ لدى الأشخاصِ الأربعة الآخرين فإن عبّرَ أحدهم بطريقةٍ ما عن مرتَّبِ شخصٍ أجنبيّ موجودٍ في الغرفةِ من دونِ ذكرِ اسمِه ، فإنَّ هذا يعدُّ نشرَ بياناتٍ شخصيَّةً عن طريقِ استخدامِ صفةٍ معيَنةٍ لا يمتلكُها شخصٌ آخرٌ في الغرفةِ و من السهلِ تحديدُه .

معالجةُ البياناتِ : هي عمليَّةُ جمعٍ أو تسجيلٍ أو تنظيمٍ أو تخزينٍ أو تعديلٍ أو استرجاعٍ أو استخدامٍ أو نشرٍ أو إزالةٍ أو تدميرِ البياناتِ الشخصيَّة بأيّ شكلٍ أو وسيلةٍ ممكنةٍ ، و تُفهَمُ بأنَّها تشمل جميع الإجراءات و الأنشطة على البيانات الشخصيَّة ، كما يمكن استخدام مصطلح "التعامل مع البينات الشخصيَّة" بدلاً من معالجةِ البيانات .

استخدامُ أسماءٍ مستعارةٍ : هي عمليةُ معالجةِ البياناتِ الشخصيَّة لجعلِها غيرَ قابلةٍ لتحديدِ شخصٍ معيَّنٍ طبيعي ، و لكن يمكنُ للمعالجِ فقط الحفاظُ على القدرةِ لربطِ البياناتِ بالشخصِ الطَّبيعيّ في حالِ اقتضَتْ الضرورةُ ذلك ، و تتضمَّنُ هذه العمليَّةُ تغييرَ معلوماتِ الهويَّةِ أو إخفائَها تماماً ، بحيثُ لا يمكنُ تعريفُ الشخصِ الطبيعيّ المعنيّ بها باستخدامِ بياناتِ المعالجةِ وحدَها .

التعريفُ العشوائيُّ : و يعني إجراءً تحوَّلُ من خلالهِ بياناتٌ شخصيَّةٌ إلى صيغةٍ لا يمكنُ استخدامُها لتحديدِ شخصٍ طبيعيٍّ ، و هذا يتمُّ عادةً عن طريقِ حذفِ العناصرِ الَّتي تمكّنُ من التعرّفِ على الأشخاص .

إنَّ استخدامَ أسماءٍ مستعارةٍ و التعريفَ العشوائيَّ إجراءانِ يهدفانِ إلى حمايةِ البياناتِ الشخصيَّةِ و إلى الحدّ من مخاطرِ التعرّفِ على الأفرادِ المعنيّينَ بالبياناتِ ، و يجري ذلكَ عن طريقِ تشفيرِ أو إخفاءِ البياناتِ القادرةِ على تحديدِ الأشخاصِ الطبيعيين .

و لذكرِ الاختلافِ بينَ المنهجيتين فإنَّ استخدامَ أسماءٍ مُستعارةٍ يجري عن طريقِ ترميزِ البياناتِ الشخصيَّةِ و لا يمكنُ الوصولُ إليها إلَّا عن طريقِ استخدامِ مفتاحِ الترميزِ ، و مالكو هذا المفتاحِ سيكونونَ قادرينَ على استخدامِ البياناتِ المرمَّزةِ لتحديدِ الأشخاصِ و التعرّفِ عليهم .

أَمَّا **التعريفُ العشوائيُّ** فإنَّه تحوَلُ البياناتِ إلى بياناتٍ فاقدةٍ للقدرةِ على تحديدِ أشخاصٍ طبيعيّين و إنْ كانَت تسمحُ بالوصولِ إلى معلوماتٍ مفيدةٍ من خلالها و لكن ليسَ لتعريفِ شخصٍ و تحديدِه .

المسؤول : هو الشخصُ الطبيعيُّ أو الجهةُ القانونيَّةُ الَّتي تحدَدُ الأغراضَ و الوسائلَ لمعالجةِ البياناتِ الشخصيَّةِ و تحديدِ سياقِ و شروطِ معالجةِ البياناتِ بما يتناسبُ مع الغرضِ من معالجتها ، كما أنَّه يتحمَّلُ مسؤوليَّةَ الامتثالِ للوائحِ الخاصَّةِ بحمايةِ البياناتِ و تنفيذَ إجراءاتٍ فعَّالةٍ لضمانِ الامتثالِ لهذهِ اللَّوائح .

و يعدُّ الالتزامُ بمبادئِ حمايةِ البياناتِ و تحقيقُ الامتثالِ لجميعِ اللَّوائحِ الخاصَّةِ بحمايةِ البياناتِ جزءاً حاسماً من دورِ المسؤولِ .

الشَّخصُ الطبيعيُّ : هو مصطلحٌ للإشارةِ إلى الأفرادِ الحقيقيّينَ الَّذينَ يمكنُ تحديدُهم بشكلٍ فرديّ ـ هذا في السياقِ القانوني ـ أمَّا في سياقِ حمايةِ البياناتِ يُستخدَمُ هذا المُصطلحُ للإشارةِ إلى الأفرادِ الأحياءِ الَّذين يتعلّقُ الأمرُ بحمايةِ بياناتِهم الشَّخصيَّةِ و حقوقِهم المتعلّقةِ بالخصوصيَّة .

معالجةُ البياناتِ بالنّيابة : هو مصطلحٌ للإشارةِ إلى عمليةِ معالجةِ البياناتِ الشخصيّةِ من قِبلِ جهةٍ أخرى غيرَ الّتي جمعَتْ البياناتِ لتحديدِ غرضِ المُعالجة .

و الجهةُ الخارجيَّةُ الَتي تقومُ بتخزينِ أو تحليلِ أو معالجةِ البياناتِ تتوجَّبُ عليها مسؤوليَّةُ حمايةِ البياناتِ الشخصيَّةِ و الالتزامُ بالمتطلَباتِ القانونيَّةِ و التنظيميَّةِ الَّتي يعرّفُها المسؤولُ أو الجهةُ المَسؤولة .

و عادةً تقسمُ إلى نوعين هما : مُلزَمة بالتعليماتِ و الأوامرِ أو غير مُلزَمة بالتعليمات و الأوامر.

و لفهمِ معنى معالجةِ البياناتِ بالنَيابةِ المُلزِمةِ بالتعليمات فهو يشيرُ إلى عمليَّة معالجةِ البياناتِ التي تتمُّ بموجب تعليمات واضحة و صريحة تُحدَّدُ من قِبلِ المسؤولِ عن معالجةِ البياناتِ .

و تُحدَّدُ المهامُ المحدودةُ و نطاقُ العملِ الَّذي يجبُ القيامُ بهِ من قِبلِ معالجي البياناتِ و التزامِهم بعدمِ تخزينِ أو إعادةِ استخدامِ هذهِ البياناتِ لأيّ غرضٍ آخرٍ ، خلافاً للتعليماتِ الصريحةِ المقدَّمةِ من المسؤولِ عن معالجةِ البياناتِ ، و عادةً ما يُبرَمُ عقدُ معالجةِ بياناتٍ يُوضّحُ الالتزاماتِ الواقعةَ على عاتقِ المعالجينَ و حقوقَ المسؤولِ عن معالجةِ البياناتِ .

و من الجديرِ ذكرُهُ أنَّه يتوجَّبُ على المسؤولِ التحقّقُ من الامتثالِ لمتطلَّباتِ الحمايةِ القانونيَّةِ و التقنيَّةِ لمعالجةِ البياناتِ ، بما في ذلكَ الإجراءاتِ الفنيَّةَ و التنظيميَّةَ والأمنيَّةَ التقنيَّةَ اللازمةَ لضمانِ سريَّةِ البياناتِ و حمايتها من الوصولِ غيرِ المصرَّحِ بهِ أو الاستخدامِ غيرِ المشروعِ ، أمَّا الشقُّ الثاني هو معالجةُ البياناتِ غيرِ الملزمةِ بالتعليماتِ ، و تكونُ معالجةُ البياناتِ الخاليةِ من التعليماتِ المقدّمةِ من المسؤولِ في حالاتِ الخدماتِ الاختصاصيَّة .

الخدمات الاختصاصيَّة : يُقصدُ بها معالجةُ البياناتِ في إطارٍ مهنيّ لبعضِ المهنِ الَّتي ترتبطُ بواجبِ الصمتِ المهنيّ وهذه المهنُ حدَّدها المشرّعُ في قائمةِ المهنِ المنتميَّةِ إلى النشاطاتِ المهنيَّةِ الحرَّةِ و هي مجدولةٌ كما يلي :

ـ مهن علاجيَّة : أطباء ، صيادلة ....

ـ مهن قانونيَّة ، استشاريَّة ، اقتصاديَّة : كالمحامين ، المستشارين ، الضرائب .

ـ المهن المتعلّقة باللغات : مترجم شفهي ، مترجم ، كتابي .

و مقدّمو الخدماتِ لمعالجةِ البياناتِ بشكلٍ خالٍ من تعليماتِ المسؤول عادةً لا يحتّمُ عليهم الالتزامَ بأيّ توجيهاتٍ من المسؤولِ عن معالجةِ البياناتِ لأنَّ الخدماتِ المهنيَّةَ الَّتي تكونُ مطلوبةً منهم تتطلَّبُ اتّخاذَ إجراءاتٍ للالتزامِ بواجبِ الصمتِ المهني .

و عادةً ما يتطلَّبُ الأمرُ الالتزامَ بمتطلَّباتِ الحمايةِ الخاصَّةِ بالبياناتِ و إجراءَ تقييمٍ للمخاطرِ و التدابيرِ الَّلازمةِ لضمانِ حمايةِ البياناتِ الشخصيَّة بشكلٍ كافٍ .

فالفرقُ الرئيسيُّ بينَ مقدّمي الخدماتِ الَّتي لا تربطُهم تعليماتٌ و الّذينَ تربطُهم تعليماتٌ تتلخَّصُ بوجودِ تعليماتٍ من الجهةِ المسؤولةِ من عدمِها ، حيثُ إنّ عدمَ وجودِ تعليماتٍ لا يُنافي الالتزامَ بالتشريعاتِ و الضوابطِ المهنيَّةِ المعمولِ بها حسبَ اللوائحِ التنظيميّةِ للمهن .

المسؤوليَّةُ المشتركةُ : وفقاً للمادَةِ (26) من الَّلائحةِ العامَّةِ لحمايةِ البياناتِ فإنَّ المسؤوليَّة المُشتركةَ تشيرُ إلى أنَه في حالِ كانَ هناكَ أكثرُ من مسؤولٍ واحدٍ لمعالجةِ البياناتِ ، فإنَّه يجبُ عليهم تحديدُ و تحقيقُ الالتزاماتِ الَّتي ينبغي عليهِم تحمُّلُها ، كما يجبُ تحديدُ المهامِ المُشتركةِ بينَ المسؤولينَ عن مُعالجةِ البياناتِ ، و كذلكَ تحديدُ الاتفاقاتِ المُناسبةِ لتنظيمِ هذه المسؤوليَّاتِ و ضمانِ التزامِ الجميعِ بالضوابطِ الخاصَّةِ بحمايةِ البياناتِ .

و يتميَّزُ المسؤولُ المُشتركُ بأنّه يتحمَّلُ المسؤوليةَ بشكلٍ مشتركٍ مع المسؤولينَ الآخرين المعنيّينَ بمعالجةِ البياناتِ الشخصيَّةِ ، و هذا يلعبُ دوراً هامَّاً حينَ يتطلَّبُ الأمرُ إجراءاتٍ منسَّقةً و موحَّدةً لحمايةِ البياناتِ و توفيرِ المعاييرِ الَّلازمةِ للخصوصيَّةِ و الأمانِ عندَ معالجةِ بياناتٍ ذاتِ حساسيَّةٍ عاليةٍ .

المُنتّدب : هو شخصٌ طبيعيٌّ يُعيَّنُ من قبلِ المسؤولِ ، و مهمَّتهُ تمثيلُ المسؤولِ في التواصلِ مع الهيئاتِ الرقابيَّةِ و تحقيقُ الالتزامِ و الامتثالِ للمتطلَّباتِ القانونيَّةِ الواقعةِ على عاتقِ المسؤولِ في حالِ كانَ مقيماً خارجَ الاتّحادِ الأوروبي .

المستلم : و هو الشخصُ الطبيعيُّ أو الجهةُ الحكوميَّةُ أو الأجهزةُ الأخرى الَّتي تتلَّقى البياناتِ الشخصيَّةَ من مسؤولِ المعالجةِ ، و يمكنُ للمستلمِ استخدامُ البياناتِ الشخصيَّةِ للأغراضِ المحدَّدةِ الَّتي جُمِعَتْ البياناتُ من أجلِها ، و لا يحقُّ للمستلمِ استخدامُها بأيّ طريقةٍ أخرى لأغراضٍ أخرى ، و يجبُ على مسؤولِ المعالجةِ أن يحدّدَ المستلمينَ الَّذينَ يمكنُهم تلقّي البياناتِ الشخصيَّةِ ، و أن يضمنَ التزامَ المستلمينَ باَّللوائحِ الخاصَّةِ بحمايةِ البيانات .

الطرفُ الثالثُ : يشيرُ هذا المصطلحُ إلى أيّ جهةٍ غيرِ المسؤولِ المعنيّ بمعالجةِ البياناتِ ، و يشاركُ في هذه المعالجةِ بشكلٍ عام ، و تعدُّ الأطرافُ الثالثةُ هي الأفرادُ أو المؤسَّساتُ أو الشركاتُ الَّتي تقومُ بمعالجةِ البياناتِ المتعلّقةِ بالأشخاصِ دونَ أن يكونَ لها علاقةٌ مباشرةٌ بالعمليّةِ الرئيسيَّةِ للمعالجة .

و من الأطرافِ الثَّالثةِ الَّتي قد تتعاملُ مع بياناتِ الأفرادِ على سبيلِ المثال :

الشركاتُ المختصَّةُ بتحليلِ البياناتِ و الإعلاناتِ على الانترنت ، و مزوّدو خدماتِ التخزينِ السَّحابيّ ، و شركاتُ الشحنِ و التوصيل .

يتوجَّبُ على المسؤولِ إعلامُ المستخدمينَ عن أيّ معاملةٍ معلوماتيَّةٍ مع الأطرافِ الثَّالثةِ ، و الحصولُ على موافقتِهم قبلَ مشاركةِ بياناتِهم .

الموافقة : و هو مصطلحٌ يشيرُ إلى موافقةِ الشخصِ على مشاركةِ بياناتِه الشخصيَّةِ من قبلِ مسؤولِ المعالجةِ ، و يعدُّ الحصولُ على موافقةٍ صريحةٍ و صالحةٍ قانونياً إذا توفَّرتْ بها ثلاثُ خصائصَ حسبَ المادَّةِ السَّابعةِ من الَّلوائحِ الأساسيَّةِ لحمايةِ البياناتِ :

أولاً : أن تكونَ الموافقةُ قابلةً للإثباتِ على سبيلِ المثالِ ، و أن تكونَ مكتوبةً و موقّعةً من صاحبِ العلاقةِ أو وكيلِهِ القانونيّ ، و لكنْ لا يُشترَطُ وجودُها بشكلٍ مكتوبٍ ، فالمهمُّ أن يكونَ المسؤولُ قادراً على إثباتِ هذه الموافقةِ .

ثانياً : أن تكونَ مفهومةً و صريحةً و تحتوي على معلوماتٍ مفصلَّةٍ عن طبيعةِ و أغراضِ معالجةِ البياناتِ الشخصيَّةِ و مدَّةِ المعالجةِ و حقوقِ الشخصِ المعنيّ بالبيانات .

ثالثاً : أن تكونَ طوعيَّةً بمعنى ألَّا يتوقّع الشخصُ المعنيُّ أيَّ أضرارٍ أو مساوئَ في حالِ عدمِ إعفاءِ الموافقةِ أو عندَ سحبِها .

و باختلالِ أي شرطٍ من الشروطِ الثلاثةِ السَّابقةِ تصبحُ الموافقةُ غيرَ صالحةٍ قانونياً أي بحكمِ الملغاة .

البيانات ذات الحساسيَّة العالية : و هي البياناتُ الَّتي حدَّدها المُشرّع في المادةِ التاسعةِ من اللوائحِ الرئيسيَّةِ لحمايةِ البياناتِ ، و تشملُ هذه الفئةُ البياناتِ العرقيَّةَ و الأصلَ العرقيَّ و المعتقداتِ الدينيَّةَ أو الفلسفيَّةَ أو التوجّهَ الجنسيَّ و الصّحةَ و البياناتِ الجينيَّةَ و الحياتيَّة .

أمَّا الفصلُ الثاني من المادةِ التاسعةِ ذكرَ الأسبابَ الَّتي تجعلُ معالجةَ هذه البياناتِ قانونياً ، و هي كما يلي:

أولاً : الموافقةُ الصريحة .

ثانياً : أن تكونَ هذهِ المعالجةُ ضروريَّةً للالتزامِ بالواجباتِ القانونيَّةِ لقانونِ العملِ و قوانينِ الحمايةِ الاجتماعيَّة .

ثالثاً : أن تكونَ معالجةُ هذهِ البياناتِ ضروريَّةً لحمايةِ المصالحِ الحيويَّةِ للشخصِ المعنيّ .

رابعاً : أن تتمَّ بناءً على أساسِ ضماناتٍ مناسبةٍ من قِبلِ مؤسَّساتٍ سياسيَّةٍ أو دينيَّةٍ أو نقابيَّةٍ في سياقِ عملِها المشروعِ ، و أن تكونَ متعلّقةً فقط بالأعضاءِ الحاليّينَ أو السابقين .

خامساً : أن يكونَ الشخصُ المعنيُّ قد نشرَها و قدَّمها للعامَّةِ بأيّ وسيلة .

سادساً : أن تكونَ هذهِ البياناتُ ضروريَّةً لإنشاءِ الدعاوى القانونيَّةِ أو ممارستِها أو الإجراءاتِ القضائيَّة .

سابعاً : أن تستندَ المعالجةُ لقانونِ الاتّحادِ الأوروبيّ أو قانونِ دولةٍ من الدولِ الأعضاءِ بما يتناسبُ مع غرضِ المعالجِ لضمانِ المصلحةِ العامَّةِ للاتّحادِ أو الدولةِ المُشرّعةِ .

ثامناً : المعالجةُ لأغراضِ الرعايةِ الصحيَّةِ أو الطبّ المهنيّ ، لتقييمِ قدرةِ العاملِ على العملِ ، بما يشملُ التشخيصَ الطبيَّ أو الرعايةَ أو العِلاج .

تاسعاً : لأسبابٍ تتعلَّقُ بالصحةِ العامَّةِ مثلَ الحمايةِ من المخاطرِ الصحيَّةِ الخطيرةِ أو لضمانِ معاييرِ الجُودةِ و السلامةِ العاليةِ في الرعايةِ الصحيَّةِ و المنتجاتِ و الأجهزةِ الطبيَّة .

عاشراً : تستندُ المعالجةُ إلى قانونِ الاتّحادِ الأوروبيّ أو دولةٍ من الدُّولِ الأعضاءِ لأغراضِ الأرشفةِ ذاتِ الأهميَّة ،أو لأغراضِ البحث العلميّ أو لأغراضٍ إحصائيَّة.

الأساسُ القانونيُّ لحمايةِ البيانات

بدايةً يجبُ أن يكونَ من المعلومِ أنَّ هيكلةَ النظامِ القانونيّ في الدولِ الأعضاءِ للاتّحادِ الأوروبيّ مختلفةٌ عن أيّ اتّحادٍ أُقيمَ بينَ أيّةِ دولٍ حيثُ أنَّ القانونَ الأوروبيَّ يعملُ كإطارٍ قانوني ينظّمُ العلاقةَ بينَ الدولِ الأعضاءِ في الاتّحادِ الأوروبيّ و يحدّدُ السلطاتِ و الاختصاصاتِ للمؤسساتِ الأوروبيَّةِ ، مثلَ المفوضيَّةِ الأوروبيَّةِ و البرلمانِ الأوروبيّ و المحكمةِ الأوروبيَّةِ ، يُنسّقُ القانونُ الأوروبيُّ مع قوانينِ الدولِ الأعضاءِ من خلالِ عمليَّةٍ تشريعيَّةٍ تشملُ المشاركةَ المتبادلةَ بينَ هذه المؤسَّساتِ و الدولَ الأعضاء .

في بعضِ الحالاتِ يصدِرُ الاتّحادُ الأوروبيُّ تشريعاً ملزِماً لجميعِ الأعضاءِ يصبحُ هذا التشريعُ جزءاً من التشريعاتِ الوطنيَّةِ في هذه الدولِ من دونِ الحاجةِ إلى تنفيذٍ محلي .

في حينِ أنَّهُ في حالاتٍ أخرى ، يتعيَّنُ على الدولِ الأعضاءِ تنفيذُ التشريعاتِ الأوروبيَّةِ في قوانينِها المحليَّةِ لتتوافقَ مع الالتزاماتِ الأوروبيَّةِ .

تشاركُ الدولُ الأعضاءُ في تشريعاتِ الاتّحادِ الأوروبيّ من خلالِ مجلسِ الاتّحادِ الأوروبيّ ، الَّذي يتكوَّنُ من وزراءِ الحكوماتِ الوطنيَّةِ في هذه الدولِ الأعضاء ، و الَّذي يناقشُ و يوافقُ على التشريعاتِ الأوروبيَّةِ المقترحة .

و بعدَ الاعتمادِ النهائيّ لهذهِ التشريعاتِ تلتزمُ الدولُ الأعضاءُ بتنفيذها و تطبيقِها في قوانينِها المحليَّةِ وفقَ جدولٍ زمنيّ و شروطٍ محدَّدةٍ في بعضِ الحالات .

و في حالِ التعارضِ بينَ التشريعاتِ الأوروبيَّةِ و قوانينِ الدولِ الأعضاءِ ، فإنَّ القانونَ الأوروبيَّ يكونُ سائداً و يجبُ تطبيقُه ، و تتوَّلى المحكمةُ الأوروبيَّةُ في بعض الأحيانِ النظرَ في التعارضاتِ القانونيَّةِ في تفسيرِ و تطبيقِ التشريعاتِ الأوروبيَّة .

و في إطارِ ما ذكرتُهُ اعتُمِدَتْ الَّلائحةُ العامَّةُ لحمايةِ البياناتِ من قِبلِ الاتّحادِ الأوروبيّ كتشريعٍ جديدٍ يتعاملُ مع حمايةِ البياناتِ في الرابعِ عشرَ من شهرِ نيسان لعامِ 2016م ، على أنْ يدخلَ حيّزَ التنفيذِ في الخامسِ و العشرينَ من شهرِ أيَّارَ لعامِ 2018م ، و الهدفُ من هذه الَّلائحةِ هو توحيدُ القوانينِ المتعلّقةِ بحمايةِ البياناتِ في جميعِ دولِ الاتّحادِ الأوروبيّ ، و تعزيزُ حقوقِ المواطنينَ بما يتعلّقُ بخصوصيَّاتهم و حمايةِ بيانَاتهم الشخصيَّة ، و تعزيزُ دعمِ التنسيقِ بينَ الدولِ الأعضاءِ فيما يتعلَّقُ بحمايةِ البيانات .

تحتوي هذه اللّائحةُ على العديدِ من العناصرِ و المبادئ على سبيلِ المثالِ لا الحصرْ و سنتعرَّفُ بشكلٍ تفصيلي على أهمّ المبادئِ في هذه اللّائحة .

الشفافية المعلوماتية : أي على المؤسَّساتِ و المنظَّماتِ توفيرُ معلوماتٍ شفَّافةٍ وواضحةٍ للأشخاصِ الَّذينَ تتعاملُ مع بياناتِهم الشخصيَّة ، بما في ذلك الغرضُ من جمعِ البياناتِ و الأساسُ القانونيُّ لذلكَ و مدَّةُ الاحتفاظِ بها و حقوقُ الأشخاصِ المعنيّينَ .

الشرعيَّةُ القانونيَّةُ لمعالجةِ البياناتِ : يجبُ على المؤسَّساتِ الاعتمادُ على أساسٍ قانونيّ مشروعٍ و شرعيّ لمعالجةِ البياناتِ الشخصيَّةِ ، و هو ما ذكرَهُ المشرّعُ بالمادةِ السادسةِ من اللّائحةِ و الأسباب و الأسس الَّتي تُعطي صفةً قانونيَّةً لمعالجةِ البياناتِ .

الموافقةُ الصريحةُ من الشخصِ المعنيّ و الَّتي تنطبقُ عليها الخصائصُ المذكورةُ في المادَّةِ السابعةِ لتكونَ صالحةً قانونيَّاً .

أو عندما تكونُ معالجةُ البياناتِ ضروريَّةً :

ـ لإتمامِ عقدٍ أو لتجهيزِ الإجراءاتِ قبلَ التعاقدِ و المقصودُ هنا على سبيلِ المثالِ :

أنَّهُ و قبلَ إبرامِ عقدٍ تُسجَّلُ بعضُ المعلوماتِ الشخصيَّةِ للشَّخصِ المعنيّ لإنجازِ مهمَّةِ الصالحِ العام .

و المعالجةُ ضروريَّةٌ لحمايةِ المصالحِ المشروعةِ للشَّخصِ المسؤولِ أو الطرفِ الثالث.

يعدَّ نموذجُ الأعمدةِ الأربعةِ في مجالِ حمايةِ البياناتِ مفهومَاً يُستخدَمُ لوصفِ مجموعةٍ من المبادئِ الأساسيَّةِ أو العناصرِ الَّتي تدعمُ أو تشكّلُ جوانبَ مختلفةً لحمايةِ البياناتِ الشخصيَّةِ و الخصوصيَّة .

تعدَّ هذهِ المبادئُ الَّلبنَةَ الأساسيَّةَ للتعاملِ مع البياناتِ الشخصيَّةِ و حمايةِ الخصوصيَّةِ، و تتكوَّنُ الأعمدةُ الأربعةُ في هذا النموذجِ من :

أولاً : الشفافيَّة و تهدفُ إلى ضمانِ أنَّ المؤسَّساتِ و الشركاتِ تقدّمُ معلوماتٍ شفافَّةً حولَ كيفيَّةِ جمعِ البياناتِ الشخصيَّةِ و استخدامِها و تخزينِها و مشاركتِها بشرطِ علمِ المستخدمينَ بأغراضِ و نطاقِ معالجةِ هذه البيانات .

ثانياً : تقييدُ أغراضِ معالجةِ البياناتِ بحيثُ تكونُ هذه الأغراضُ محدَّدةً و مشروعةً مع وجوبِ عدمِ معالجةِ البياناتِ من دونِ وجودِ موافقةٍ للشَّخصِ المعنيّ بأغراضٍ أخرى .

ثالثاً : تحديدُ مدى البياناتِ : يُوصى بجمعِ و استخدامِ البياناتِ الشخصيَّةِ الَّلازمةِ فقط لإنجازِ الهدفِ من المعالجةِ مع وجوبِ تجنُّبِ جمعِ بياناتٍ زائدةٍ أو غيرِ ضروريَّة .

رابعاً : أمانُ البياناتِ إذ يجبُ اتّخاذُ تدابيرَ تقنيَّةٍ و تنظيميَّةٍ لضمانِ حمايةِ البياناتِ الشخصيَّةِ من الوصولِ غيرِ المصرّحِ به أو الفقدانِ أو الاستخدامِ السيء .

يعملُ نموذجُ الأعمدةِ الأربعةِ كإطارٍ لضمانِ حمايةِ البياناتِ الشخصيَّةِ و تعزيزِ التعاملِ المشروعِ و المسؤولِ مع هذه البياناتِ كما أنَّهُ يسهمُ في بناءِ ثقةِ المستجدّينَ في حمايةِ البياناتِ و الحفاظِ على خصوصيَّتهم.

في سياقِ حمايةِ البياناتِ ، يمكنُ تحديدُ عدَّةِ فئاتٍ للبياناتِ ، تستخدمُ هذهِ الفئاتُ لتصنيفِ البياناتِ الشخصيَّةِ وفقًا لنوعِها وحساسيَّتها ، و فيما يلي بعضُ فئاتِ البياناتِ الشائعةِ :

1- بياناتُ الهويَّةِ: تشملُ معلوماتٍ مثلَ الاسمِ، و العنوانِ ، و تاريخِ الميلادِ ،و الرقمِ التأمينيّ الاجتماعِي وغيرِها من البياناتِ الَّتي تُستخدَمُ لتحديدِ هويَّةِ الشخصِ بشكلٍ فريد .

2- بيانات الاتّصالِ: تشملُ معلوماتٍ مثلَ أرقامِ الهاتفِ وعناوينِ البريدِ الإلكترونيّ وغيرِها من معلوماتِ الاتّصالِ الَّتي تُستخدَمُ للتّواصلِ مع الشخصِ

3- بياناتٌ ماليَّةٌ : تشملُ أرقامَ حساباتِ البنوكِ، و معلوماتِ بطاقاتِ الائتمانِ ، و بياناتِ الرواتبِ وغيرِها من التفاصيلِ الماليَّةِ للشّخصِ .

4- بياناتٌ صحيَّةٌ : تشملُ معلوماتٍ عن الحالة الصحيَّةِ للشّخصِ ، والتشخيصاتِ الطبيَّةَ ، و التاريخَ الطبيّ ، و الأدويةَ الموصوفةَ ومعلوماتٍ طبيَّةٍ حسَّاسةٍ مماثلةٍ .

5- بياناتُ الموقعِ : تشملُ معلوماتٍ عن موقعِ الشخصِ الحاليّ أو الماضي ، الَّتي يمكن تتبعها عبر تقنيات و أبراجِ الهاتفِ المحمولِ (GPS) مثل نظام تحديد المواقع العالمي و غيرِها .

6- بياناتٌ حيويَّةٌ : تشملُ معلوماتٍ حيويَّةً أو فيزيولوجيَّةً مثلَ بصماتِ الأصابعِ، و مسحِ العينِ ، و التعرّفِ على الوجهِ وميزاتٍ أخرى يمكنُ استخدامُها لتحديدِ هويَّةِ الشخصِ بشكلٍ فردي .

و من المهمِ أن نلاحظَ أنَّ هذهِ مجرَّدُ أمثلةٍ لفئاتِ البياناتِ ، وقد تكونُ هناكَ فئاتٌ أخرى محدَّدةٌ تعتمدُ على سياقِ ونطاقِ حمايةِ البياناتِ المعني .

و أذكرُ هنا بعضَ الأمثلةِ على المبرّراتِ القانونيَّةِ لإتمامِ عقدٍ مبرمٍ في حمايةِ البياناتِ :

1.معالجةُ البياناتِ الشخصيَّةِ الَّلازمةِ لإبرامِ وتنفيذِ عقدِ الشراءِ ، على سبيلِ المثالِ عندما يقومُ شخصٌ بطلبِ منتجٍ عبرَ الإنترنت ، يتعيَّنُ معالجةُ بياناتِه الشخصيَّةِ مثلَ الاسمِ ، والعنوانِ ، ومعلوماتِ الدفعِ لتنفيذِ العقدِ و توصيلِ الطلبِ .

2.معالجةُ البياناتِ الشخصيَّةِ في إطارِ عقدِ العملِ ، إذ يجبُ معالجةُ بياناتِ الموظفينَ مثلَ معلومات الاتّصالِ وتفاصيلِ الحسابِ المصرفيّ ورقمِ الضمانِ الاجتماعيّ لتنفيذِ عقدِ العملِ والامتثالِ للالتزاماتِ القانونيَّةِ المتعلّقةِ بالعملِ .

في كلا الحالتينِ ، تكونُ معالجةُ البياناتِ الشخصيَّةِ ضروريَّةً لتنفيذِ العقدِ وهذا يشكّلُ أساساً قانونيّاً لمعالجةِ البياناتِ الشخصيَّةِ وفقاً للقوانينِ واللوائحِ الخاصَّةِ بحمايةِ البيانات .

أضيفُ هنا بعضَ الأمثلةِ على المبرّراتِ القانونيَّةِ للامتثالِ للالتزاماتِ القانونيَّةِ في حمايةِ البيانات :

1- الالتزاماتُ الضريبيَّة: يكونُ من الواجبِ القانونيّ على الشركاتِ تجميعُ ومعالجةُ بعضِ البياناتِ الشخصيَّةِ للموظَّفينَ والعملاءِ من أجلِ الامتثالِ للتعليماتِ الضريبيَّة .

2- الامتثالُ لمتطلباتِ الجهاتِ الرقابيَّةِ : يجبُ على المؤسَّساتِ الماليَّةِ معالجةُ البياناتِ الشخصيَّةِ لعملائِها للامتثالِ لمتطلباتِ الجهاتِ الرقابيَّةِ في قطَّاعِ الخدماتِ الماليَّةِ ، مثلَ تقديمِ تقاريرَ عن حالاتِ الشبهاتِ المتعلّقةِ بغسلِ الأموالِ .

3- الالتزاماتُ بالاحتفاظِ بالسجلاتِ : هناكَ بعضَ القطَّاعاتِ الَّتي تفرضُ على الشركاتِ الالتزامَ بالاحتفاظِ ببعضِ البياناتِ الشخصيَّةِ لفترةٍ زمنيَّةٍ محدَّدةٍ ، و يمكن أن يشمل ذلك على سبيل المثال ، سجلَّاتٍ طبيَّةً أو وثائقَ قانونيَّة .

4- الامتثالُ لإجراءاتٍ قانونيَّةٍ: في بعضِ الإجراءاتِ القانونيَّة، قد يكونُ من الضروريّ معالجةُ بياناتٍ شخصيَّةٍ للامتثالِ لالتزاماتٍ قانونيَّةٍ ، مثلَ أوامرِ المحكمةِ أو التحقيقاتِ الرسميَّة .

توضّحُ هذهِ الأمثلةُ أنَّ معالجةَ البياناتِ الشخصيَّةِ قد تكونُ مبرَّرةً قانونيّاً عندما تكونَ ضروريَّةً من أجلِ الامتثالِ للالتزاماتِ القانونيَّة ، ومع ذلكَ فمنَ المهمّ التأكُّدُ أنَّ المعالجةَ تتمُّ وفقاً للقوانينِ واللَّوائحِ الخاصَّةِ بحمايةِ البياناتِ .

و ختاماً أودُّ ذكرَ بعضِ الأمثلةِ على المبرّراتِ القانونيَّة لموازنةِ المصالحِ في حمايةِ البيانات :

1- التسويق المباشر: يمكنُ للشركاتِ معالجةُ البياناتِ الشخصيَّةِ لأغراضِ التسويقِ المباشرِ، استناداً إلى المصلحةِ المشروعةِ في تقديمِ منتجاتِها أو خدماتِها للعملاءِ المُحتمَلين ، ومع ذلكَ من المهمّ ضمانُ احترامِ حقوقِ خصوصيَّة الأفرادِ ، وحمايةُ خصوصيَّاتهم بشكلٍ مناسب .

2- المراقبةُ بالفيديو: في بعضِ الحالاتِ ، يمكنُ للمؤسَّساتِ استخدامُ المراقبةِ بالفيديو لضمانِ سلامةِ الموظَّفينَ أو العملاءِ أو الممتلكاتِ ، و يمكنُ تبريرُ ذلكَ بناءً على المصلحةِ المشروعةِ في منعِ السرقةِ أو التخريبِ أو أنشطةٍ غيرِ قانونيَّة أخرى. ومع ذلكَ ، يجبُ مراعاةُ مبادئِ التناسبِ والشفافيَّةِ في ذلك .

3- مراقبةُ الموظّفين : قد يقومُ أربابُ العملِ بمراقبةِ بعضِ البياناتِ الشخصيَّةِ للموظَّفين لضمانِ الالتزامِ بساعاتِ العملِ ، أو سلامةِ مكانِ العملِ ، أو أمانِ تقنيَّةِ المعلومات ، و يمكنُ تبريرُ ذلكَ بناءً على المصلحةِ المشروعةِ في بيئةِ عملٍ فعَّالةٍ وحماية مواردِ الشركةِ ، ومع ذلك يجبُ مراعاةُ حقوقِ وخصوصيَّة الموظَّفينَ بشكلٍ مناسب .

4- نقلُ البياناتِ داخلَ مجموعةِ الشركات: في حالةِ الشَّركاتِ متعددةِ الجنسيَّات، يمكنُ تبريرُ نقلِ البياناتِ الشخصيَّةِ بينَ الشركاتِ التابعةِ المختلفةِ ، بناءً على المصلحةِ المشروعةِ في إدارةٍ فعَّالةٍ لمجموعةِ الشَّركاتِ ، و يجب ضمانُ اتّخاذ تدابيرَ أمنيَّةٍ مناسبةٍ لحمايةِ البياناتِ الشخصيَّة ، و ضمانِ عدمِ الوصولِ إليها بشكلٍ غير قانوني .

مستوياتُ حماية البياناتِ حسب النموذجِ الاتحادي

مفهوماً في مجالِ حمايةِ البياناتِ يعدُّ النموذجُ الَّذي يعتمِدُ على مستوياتِ الحمايةِ

و يهدف إلى تعريفِ وضمانِ الحمايةِ المناسبةِ للبياناتِ ، و يحدّدُ هذا النموذجُ الإجراءاتِ الأمنيَّةَ والتدابيرَ الواجب اتّخاذُها لمختلفِ مستوياتِ حمايةِ البيانات .

و غالباً ما يستندُ النموذجُ الَّذي يعتمدُ على مستوياتِ الحمايةِ إلى تقييمِ المخاطرِ والحساسيَّةِ للبياناتِ ، و يمكن أخذُ معاييرَ مختلفةٍ في الاعتبارِ ، مثل الضررِ المحتملِ في حالةِ فقدانِ البياناتِ أو الكشفِ عنها ، وتأثيرها على خصوصيَّةِ الأشخاصِ المعنيّينَ والمتطلَّباتِ القانونيَّةِ .

وعادةً تُحدَّدُ مستوياتُ الحمايةِ على شكلِ هرمٍ أو تسلسلٍ ، مثلَ منخفضٍ ومتوسّطٍ وعالي ، و كلَّما زادَ مستوى الحمايةِ ، كلَّما كانَتْ متطلَّباتُ الأمانِ والتدابيرُ الَّلازمةُ أكثرَ صرامةً لحمايةِ البياناتِ .

يعملُ النموذجُ الَّذي يعتمدُ على مستوياتِ الحمايةِ كدليلٍ للمنظَّماتِ من أجلِ ضمانِ الامتثالِ لحمايةِ البياناتِ وفقاً لحساسيّةِ البياناتِ ، وتنفيذِ التدابيرِ الأمنيَّةِ المناسبةِ ، كما يساعدُ في تقييمِ المخاطرِ وتحديدِ الأولويَّاتِ في تنفيذِ إجراءاتِ حمايةِ البياناتِ

و من المهمِ أن نلاحظَ أنَّ النموذجَ الَّذي يعتمِدُ على مستوياتِ الحمايةِ قد يختلفُ من منظَّمةٍ إلى أُخرى، وذلكَ اعتماداً على المتطلَّباتِ والسياقاتِ الخاصَّةِ بها .

و في نموذجِ الحمايةِ الألمانيّ في مجالِ تكنولوجيا المعلوماتِ يُعيَّنُ كلُّ مستوىً لتحديدِ متطلَّباتٍ وإجراءاتٍ محدَّدةٍ لضمانِ أمانِ تكنولوجيا المعلومات ، و فيما يلي شرحٌ موجزٌ لكل مستوى :

1- مستوى الحماية A (مستوى حماية منخفض): ينطبقُ هذا المستوى على الأنظمةِ والبياناتِ الَّتي لديها احتياجاتُ حمايةٍ منخفضة ، و يتمُّ التركيزُ على تأمينِ النظامِ الأساسيّ ضدَ التهديداتِ والمخاطرِ المعروفة.

2- مستوى الحماية B (مستوى حماية أساسي): ينطبقُ هذا المستوى على الأنظمةِ والبياناتِ الَّتي لديها احتياجاتُ حمايةٍ متوسّطة ، و تُتَّخذُ تدابيرُ أمانٍ متقدّمة للحمايةِ من التهديداتِ الشائعةِ .

3ـ مستوى الحماية C (مستوى حماية مرتفع): ينطبقُ هذا المستوى على الأنظمةِ والبياناتِ الَّتي لديها احتياجاتُ حمايةٍ عالية ، و يتطلَّبُ اتّخاذَ تدابيرِ أمانٍ إضافيَّةٍ للوقايةِ من التهديداتِ الشائعةِ والتهديداتِ الخاصَّة .

4ـ مستوى الحماية D/E (مستوى حماية عالي): ينطبقُ هذا المستوى على الأنظمةِ والبياناتِ الحسَّاسةِ للغاية ، والَّتي تتطلَّبُ حمايةً عالية ، و تُتَّخذُ تدابيرُ أمانٍ شاملةٌ ومتقدّمةٌ للوقايةِ من الهجماتِ المستهدفةِ والتهديدات المتقدمة .

و تعمل هذه المستويات كمرشد لتحديد المعايير الأمنيَّة المطلوبة واتّخاذ التدابير اللازمة .

يعدُّ هذا التحليلُ أسلوباً في حمايةِ البياناتِ إذ يهدفُ إلى تعريفِ وتقييمِ الأهدافِ الأساسيَّةِ لأمانِ المعلوماتِ ، وتحديدِ التدابيرِ الواجبِ اتّخاذها ، و يُعد هذا المفهومُ منتشراً على نطاقٍ واسعٍ لتحليلِ متطلَّباتِ الأمانِ للبياناتِ والأنظمةِ وتحديدِ التدابيرِ الأمنيَّةِ المناسبة .

يتكوّن تحليل CIA من الآتي:

1- **السريَّة** : تتعلَّق بحمايةِ المعلوماتِ من الوصولِ غيرِ المصرَّحِ به أو الكشفِ عنها ، و يتضمَّنُ ذلكَ حمايةَ البياناتِ الحسَّاسةِ من الإطّلاعِ غيرِ المصرَّحِ به من قِبلِ أطرافٍ ثالثة ، و تتضمَّنُ التدابيرَ المتَّخذةَ لضمانِ السريَّة استخدامَ تقنيَّاتِ التشفيرِ، وضوابطَ الوصولِ ، وسياساتِ أمانِ البيانات.

2- **النزاهة** : تتعلَّقُ بضمانِ صحَّةِ وكماليَّةِ البياناتِ ، و يتعلَّقُ الأمرُ بضمانِ حمايةِ البياناتِ من التعديلِ غيرِ المصرَّح به ، أو التلاعبِ ، أو التلفِ ، و تشملُ التدابيرُ المتَّخذةُ لضمانِ النزاهةِ استخدامَ علاماتٍ للتحقّق ، والتوقيعات الرقميَّة ، ومراقبةَ الإصدارات ، ونسخَ البيانات.

3- **التوفر** : يتعلَّقُ بإمكانيَّة الوصولِ إلى المعلوماتِ والأنظمةِ في الوقتِ المناسبِ والمكانِ المناسبِ ، و يتعلَّقُ الأمرُ بضمانِ توفّرِ البياناتِ والأنظمةِ بشكلٍ مستمر وحمايتها من الاضطراباتِ أو الأعطالِ ، و تشملُ التدابيرُ المتَّخذةُ لضمانِ التوفر تطبيقَ الاحتياطيات ، وخططَ الاستعادةِ من الطوارئ، والصيانةِ والمراقبةِ المنتظمةِ.

و يعملُ هذا التحليلُ كإطارٍ لتقييمِ متطلَّباتِ الأمانِ واختيارِ التدابيرِ الواجبِ اتّخاذُها من خلالِ تحليلِ السريَّةِ ، والنزاهةِ ، والتوفرِ، و يمكنُ للمؤسَّساتِ تطويرُ استراتيجياتِ أمانِها وتنفيذِها لضمانِ الخصوصيَّةِ وحمايةِ المعلوماتِ الحسَّاسةِ .

يتعلَّق تحليلُ المخاطرِ في حمايةِ البياناتِ بعمليَّةِ تحديدِ وتقييمِ وتقديرِ المخاطرِ المحتملةِ المتعلّقةِ بمعالجةِ البياناتِ الشخصيَّة ، إنَّها جزءٌ مهمٌّ من إجراءاتِ حمايةِ البياناتِ ، وتهدفُ إلى منعِ أو تقليلِ انتهاكاتِ الخصوصيَّةِ وفقدانِ البياناتِ .

يتضمَّنُ تحليلُ المخاطرِ في حمايةِ البياناتِ الخطواتِ التالية :

1- **تحديدُ البياناتِ الشخصيَّةِ** : إذ يجب تحديدُ جميعِ البياناتِ الشخصيَّةِ الَّتي تُعالّجُ في المؤسَّسة.

2- **تقييمُ الأنشطةِ المعالجة** : يتمُّ بعد ذلكَ تقييمِ الأنشطةِ المختلفةِ للمعالجةِ الَّتي تستخدمُ أو تعالجُ البياناتِ الشخصيَّة ، وهذا يشملُ على سبيلِ المثالِ جمعَ البياناتِ وتخزينّها ونقلِها أو حذفها .

3- **تحديدُ المخاطرِ** : يتمُّ تحديدُ المخاطرِ المحتملةِ والتهديداتِ الَّتي قد تنشأُ عن الأنشطةِ المعالجةِ ، و يمكنُ أن تشملَ هذه المخاطرُ ، المخاطرَ التقنيَّة مثلَ تسريبِ البياناتِ أو هجماتِ الاختراق ، وكذلكَ المخاطرَ غيرَ التقنيَّةِ مثلَ الأخطاءِ البشريَّةِ أو الصلاحياتِ غيرِ السليمة .

4- **تقييمُ المخاطر** : يتمُّ تقييمُ المخاطرِ لتحديدِ آثارِها واحتماليَّةِ حدوثِها ، وبذلكَ يمكنُ تحديدُ المخاطرِ الرئيسيَّة الَّتي تستدعي اهتماماً خاصَّاً.

5- **تدابير التقليل من المخاطر**: بناءً على المخاطرِ المحدَّدةِ والَّتي تمَّ تقييمها ، تُوضَعُ التدابيرُ المناسبةُ للتقليلِ من المخاطرِ ، و يمكنُ أن يشملَ ذلكَ تنفيذَ التدابيرِ الأمنيَّةِ التقنيَّةِ ، وتدريبَ الموظَّفينَ ووضعَ السياساتِ والإجراءاتِ و آليات التحكم الأخرى.

6- **المراقبةُ و التحديث** : يجبُ مراجعةُ تحليلُ المخاطرِ بانتظام وتحديثه ، حيثُ يمكنُ أن تتغيرَ المخاطرُ مع مرورِ الوقت ، من المهم التأكدُ أنَّ التدابيرَ المتَّخذة لا تزالُ فعَّالة وتلبّي المتطلَّباتِ الحالية .

و إجراءُ تحليلِ المخاطرِ في حمايةِ البياناتِ يساعدُ المؤسَّساتِ على اكتشافِ نقاطِ الضعفِ المحتملةِ فيما يتعلَّقُ بحمايةِ البياناتِ واتّخاذِ التدابيرِ المناسبةِ لتقليلِ هذه المخاطرِ ، وبذلك يمكنُها ضمانُ سريَّة وسلامةِ وتوفرِ البياناتِ الشخصيَّةِ والامتثال للقوانينِ واللَّوائحِ الخاصَّةِ بحمايةِ البيانات .

أكبرُ مجموعِ غراماتٍ فُرضَتْ على شركةٍ أمريكيَّةٍ !

فرضَ الاتّحادُ الأوروبيّ غرامةً قياسيَّةً على شركةِ (ميتا) ، وهي الشركةُ الأم لفيسبوك ، بسببِ تحويلِ بياناتِ المستخدمينَ إلى الولايات المتّحدة ، وطُلبَ أيضاً من (ميتا) وقفَ نقلِ البيانات ، و حذَّرَ اتّحادُ الصناعاتِ الرقميَّةِ "بيتكوم" بأنَّ أوروبَّا لا ينبغي أن تفرضَ حجباً على البيانات .

اتّخذَ الاتّحادُ الأوروبيّ إجراءاتٍ حازمةً في نزاعٍ حولَ حمايةِ البياناتِ مع شركةِ (ميتا) ، وهي الشركةُ المالكةُ لفيسبوك ، وذكرَتْ لجنةُ حمايةِ البياناتِ الإيرلنديَّة ، الَّتي تتولَّى شؤونَ الشركةِ ، أنَّها فرضت غرامةً قيمتُها /1.2/ مليار يورو على شركةِ (ميتَّا) بسببِ انتهاكِها للوائحِ حمايةِ البياناتِ الأوروبيَّةِ (DSGVO).

تتعلَّقُ الخلفيَّةُ بنزاعٍ يدورُ منذُ سنواتٍ بشأنِ نقلِ بياناتِ مستخدمي فيسبوك من الاتّحادِ الأوروبيّ إلى خوادمَ في الولايات المتَّحدة ، وقد أعطّتْ لجنةُ حمايةِ البياناتِ الإيرلنديَّة (DPC) لشركةِ (ميتا) خمسةَ أشهرٍ لمنعِ نقلِ البياناتِ إلى الولايات المتَّحدة ، وكان السببُ وراءَ ذلكَ هو شكوى من قبلِ الناشطِ النمساوي لحمايةِ البياناتِ (ماكس شريمس) ، إذ يرتبطُ الأمرُ بمخاوفَ من أنَّ وكالاتِ المخابراتِ الأمريكيَّةَ قد تتمكَّنُ من الوصولِ إلى معلوماتِ مستخدمينَ أوروبيّين ، فقام شريمس في ذلكَ الوقتِ بتقديمِ شكوى ضدَ فيسبوك ، و ينطبقُ القرارُ الحاليُّ فقط على هذه الشبكةِ الاجتماعيَّة ، ولا يشملُ خدماتٍ أخرى تابعةٍ لمجموعةِ (ميتا) مثل انستغرام أو واتساب .

رفضَتْ هيئةُ حمايةِ البياناتِ الإيرلنديَّة DPC لسنواتٍ طويلةٍ التصدّي للقضيةِ ضدَ فيسبوك ، وفي النهايةِ ألزَمَتْ المجلسَ الأوروبيَّ لحمايةِ البياناتِ (EDSA) هيئة DPC بفرضِ عقوبةٍ على شبكةِ التواصل الاجتماعي .

كانت هيئةُ DPC فرضَتْ بالفعلِ غرامةً بقيمةِ /390/ مليون يورو على شركةِ (ميتا) في يناير بسببِ إجبارِ مستخدمي فيسبوك وانستغرام للموافقةِ على الإعلاناتِ المستهدفةِ ، وحتَّى الآن فُرِضَتْ غراماتٌ بقيمةِ /4/ مليار يورو على (ميتا) منذُ بدءِ تنفيذِ اللَّائحةِ الأوروبيَّة لحمايةِ البياناتِ قبلَ خمسِ سنوات .

أحدُ أهمّ المبادئِ الأساسيَّةِ في حمايةِ البياناتِ هو مبدأُ الارتباطِ بالغرضِ ، وفقًا لهذا المبدأ، يجبُ جمعُ البياناتِ الشخصيَّةِ واستخدامِها ومعالجتِها فقط إذا كانَ ذلكَ يخدمُ غرضاً محدَّداً حُدّدَ مسبقاً بوضوح ، يعطي المتقدّمونَ للوظائفِ موافقتَهم على ذلكَ عن طريقِ إرسالِ الطلبِ عادةً .

تحدّدُ حمايةُ البياناتِ أيضاً أنَّهُ بعدَ تحقيقِ الغرضِ ، و يجبُ ألا تكونَ البياناتُ متاحةً بعد الآنِ ، و عادةً ما يتطلَّبُ ذلكَ حذفَ البياناتِ .

و وفقاً لحمايةِ البياناتِ ، يجوزُ الاحتفاظُ بطلبِ التوظيفِ طالما أنَّ الوظيفةَ المعلنَ عنهَا لم تُشغَلْ بعد ، وحفظُ بياناتِ المتقدّمينَ لفترةٍ أطولَ يكونُ غالباً ما يكونُ غيرَ مسموحٍ به ، إذا لم يكُنْ المنصبُ المعلنُ عنه متاحاً بعدَ الآن ، و يجبُ على الشركاتِ حذفُ جميعِ بياناتِ المتقدّمينَ المقدَّمةِ لذلكَ ما لم يعطي المتقدّمُ موافقةً بشروطٍ مختلفةٍ ، وتشملُ هذه أيضاً جميعَ المعلوماتِ من مقابلةِ العمل (الملاحظات).

إذا وصلَتْ ملفاتُ التقديمِ بالبريدِ العاديّ ، فيجبُ إعادتُها إلى المتقدّمِ في غضونِ شهرينِ إلى ثلاثةِ أشهرٍ في أقصى الحالاتِ ، ما لم يُتَّفَقْ على إتلافِها بشكلٍ صحيحٍ ومناسب .

يتماشى الإجراءُ المشابهُ أيضاً مع حمايةِ البياناتِ عندما يُحتَفَظُ بطلبِ توظيف ، سواءً كانَ مقدَّماً بالكتابةِ أو عبرَ البريدِ الإلكتروني ، بموافقةٍ صريحةٍ من المتقدّمِ لفترةٍ تتخطَّى دورةَ التوظيفِ ، و يُحتَفَظُ به أو يُخزَّن .

أمَّا التقديمُ عبرَ البريدِ الإلكترونيّ أصبحَ في الوقتِ الحاليّ منتشراً في العديدِ من المجالاتِ الاقتصاديَّة ، و يمكنُ بسهولةٍ توزيعُ طلباتِ التوظيفِ عبرَ الإنترنت لمزيدٍ من الأشخاصِ المخوَّلينَ للنظرِ فيها ، ومع ذلكَ يُعدُّ الحذفُ المنتظمُ للبياناتِ المقدَّمةِ عبرَ الإنترنت مشكلةً فيما يتعلَّقُ بحمايةِ البيانات ..

و يجبُ على جميعِ الأفرادِ والشركاتِ المعنيّينَ أن يكونوا على علمٍ بأنَّ جميعَ النسخِ والبريدَ الإلكترونيَّ والطباعاتِ المتعلّقةِ بطلبِ التوظيفِ يجبُ حذفُها أو تدميرُها بعدَ تحقيقِ الغرضِ المحدَّدِ ، قد يتطلَّبُ هذا تدريباً مناسباً لتجنّبِ وضعِ بياناتِ المتقدّمينَ غير المخوَّلةِ في أي ملفٍ على الكمبيوتر ، ويُعدُّ ذلكَ انتهاكاً لحمايةِ البياناتِ ، لذا يجبُ التعاملُ بعنايةٍ خاصَّةٍ مع البياناتِ الخاصَّةِ بطلباتِ التوظيفِ .

وفقًا لقانونِ حمايةِ البياناتِ الألماني (BDSG) يجوزُ لأربابِ العملِ تخزينُ بياناتِ الموظَّفين ومعالجتِها فقط إذا كانَتْ ضروريَّةً لتنفيذِ علاقةِ العملِ ، تشملُ هذهِ البياناتُ بشكلٍ رئيسيّ بياناتِ الموظَّفينَ الأساسيَّةِ ومعلوماتٍ حولَ التعليمِ والمؤهّلاتِ المهنيَّةِ ، إذ يجبُ على أربابِ العملِ إبلاغُ موظَّفِيهم عن معالجةِ بياناتِهم ، و يمكنُ أنْ يكونَ ذلك إمَّا في عقدِ العملِ أو في ورقةِ معلوماتٍ خاصَّةٍ.

يجوزُ إعادةُ إرسالِ بياناتِ الموظَّفينَ أيضاً إلى مستشارِ الضرائبِ أو مكتبش المرتَّباتِ لمعالجةِ البياناتِ .

متى تكونُ الموافقةُ على معالجةِ البياناتِ ضروريَّة ؟

إذا أرادَ صاحبُ العملِ معالجةَ بياناتٍ إضافيَّةٍ للموظَّفينَ الَّتي لا تندرجُ ضمنَ هذا النطاقِ أو معالجةِ بياناتِ الموظَّفينَ لأغراضٍ أخرى ، فإنَّه يحتاجُ وفقاً لِّلوائحِ الأساسيَّةِ إلى موافقةٍ محدَّدةٍ من الموظَّف ، و يمكنُ أن يحدثَ ذلكَ على سبيلِ المثالِ في حالةٍ قائمةٍ بأعيادِ الميلادِ أو عندما تضعُ الصورَ الخاصَّةَ بالموظَّفينَ على موقعِ الشركةِ على الإنترنت ، و من المهمّ هنا أنْ يقدّمَ الموظَّفُ موافقتَه بشكلٍ طوعي - وعادةً ما يُكتَبُ ذلك ، وبهذا يكونُ لدى صاحبِ العملِ دليلٌ مناسبٌ على ذلك .

كما أنَّهُ في المبدأ ، يجوزُ للشركاتِ تسجيلُ أوقاتِ العملِ للموظَّفينَ ، حيثُ تشكّلُ غالباً أساساً لأجرِ العملِ ، وإذا كانَ أحدُ الموظَّفينَ مشمولاً بقانونِ الحدّ الأدنى للأجورِ ، فيجبُ تسجيلُ مدَّةِ العملِ اليوميَّةِ بشكلٍ إلزاميّ .

أمَّا طريقةُ تسجيلِ أوقاتِ العملِ (الساعات التلقائية، تطبيقات الويب، إلخ)، فيتركُ ذلكَ بشكلٍ كبيرٍ لصاحبِ العملِ ، ومع ذلكَ يجبُ على صاحبِ العملِ أنْ يضمنَ أنَّهُ يحتفظُ ببياناتِ ساعاتِ العملِ فقط لمدَّةِ الوقتِ الَّلازمِ لتنفيذِ علاقةِ العملِ ، وبشكلٍ عامٍ ، يُسمَحُ بالاحتفاظِ بتلكَ البياناتِ لمدَّةِ عامين .

يجوزُ لصاحبِ العملِ الاطّلاعُ على حساباتِ البريدِ الإلكترونيّ الخاصَّةِ بالشركةِ بشكلٍ محدود.

و إذا قدَّمَتْ الشركةُ حساباتِ بريدٍ إلكترونيّ لموظَّفيها، يجوزُ استخدامُها فقط لأغراضِ العمل ، و في حالةِ الاستخدامِ تُصرَفُ للأغراضِ العمليَّةِ ، و يكونُ لدى صاحبِ العملِ حقُّ اطّلاعٍ محدودٍ : إذ يجوزُ له قراءةُ رسائلِ البريدِ الإلكترونيّ وتمكينُ موظَّفينَ آخرينَ من استخدامِ حساباتِ البريدِ الإلكترونيّ الخاصَّةِ بالشركة ، و الشرطُ هو أنْ تجعلَ الظروفَ العمليَّةَ هذا ضروريَّاً ، و يكونُ ذلكَ الحال مثلاً عندما يتغيَّب موظَّفٌ بسببِ المرضِ أو في عطلةٍ لفترةٍ طويلة .

و لكي يستمرَ العملُ في نفسِ النمطِ المعتادِ ، يجبُ على الموظَّفينَ الغائبينَ أن يكونوا على درايةٍ أنّه عند الغياب الطويلِ عن العمل يمكن أن تُعالَجَ رسائلُ البريدِ الإلكترونيّ أيضاً من قِبلِ موظَّفينَ آخرين ، ومن أجلِ ضمانِ ذلكَ، يجوزُ لصاحبِ العملِ الوصولُ إلى حساباتِ البريدِ الإلكترونيّ الخاصَّةِ بالشركةِ للموظَّفينَ الغائبين .

علاوةً على ذلك ، يُسمَحُ لصاحبِ العملِ الوصولُ إلى حساباتِ البريدِ الإلكترونيّ الخاصَّة بالشركةِ عشوائياً للقيامِ بإجراءاتِ مراقبةٍ أو تقييماتِ الأداء ، ولكن يكونُ ذلكَ قانونيَّاً فقط إذا أُبلِغَ الموظَّفونَ مسبقاً بأنَّ تلكَ التدابيرَ التجسُّسيَّةَ ستُجرى وبأيّ مدىً ستتمُّ ، و يمكنُ أن يكونَ الإعلامُ عن ذلكَ أيضاً في شكلِ اتفاقيَّةِ الشركةِ

و تُحظَرُ المراقبةُ النظاميَّةُ والمتواصلة : إذ يجبُ على صاحبِ العملِ أن يكونَ لديه دائماً أساسٌ قانونيٌّ لإجراءاتِ المراقبةِ ويجبُ أن يُفحصَ إذا كانَ هناك وسائلُ أكثرَ اعتدالاً ، متاحة لتحقيقِ نفسِ الأهدافِ (المحكمة الأوروبية لحقوق الإنسان).

كما أنَّ صاحبَ العملِ ممنوعٌ من قراءةِ رسائلِ البريدِ الإلكترونيّ الخاصَّةِ إذا لم تعطى موافقة مسبقة صالحةٌ قانونيَّاً ، تُوجَّهُ بعقدِ العملِ لاستخدامِ البريدِ الإلكترونيّ الخاصّ بالشركةِ للأغراضِ الشخصيَّة ، فإنَّ ذلكَ يكونُ ممنوعاً ، ولكنَّ هذا لا يعني أنَّ صاحبَ العملِ يجوزُ له في إطارِ حقّ الوصولِ المحدودِ له قراءةُ رسائلِ البريدِ الإلكترونيّ الشخصيَّة الَّتي تُرسَل أو تُستقبَل عبرَ البريدِ الإلكترونيّ الخاص بالشركةِ سواءً كانتْ مسموحةً أو لا ، فإنَّ وصولَ صاحبِ العملِ إلى رسائلِ البريدِ الإلكترونيّ الشخصيَّةِ ممنوعٌ

في كلّ الأحوالِ لأنَّهُ بذلك ينتِهكُ حقوقَ شخصيَّةِ الموظَّفين ، في حالةِ التجاوزِ عن هذا الأمرِ، و تهدّدُ صاحبَ العملِ عواقبُ جنائية. لذلكَ ينبغي للموظَّفينَ تسميةُ رسائلِ البريدِ الإلكترونيّ الشخصيَّةِ بأنَّها كذلكَ لاستبعادِ مخاطرِ قراءتِها من قبلِ صاحبِ العملِ ، و يُسمَحُ عادةً بتبادلِ بعضِ رسائلِ البريدِ الإلكترونيّ الشخصيَّة عبرَ البريدِ الإلكترونيّ الخاصّ بالشركةِ ، ولكنْ إذا استُخدِمَتْ بانتظامٍ للأغراضِ الشخصيَّةِ ، فقد يؤدّي ذلكَ إلى تحذيراتٍ وحتَّى إنهاءِ عقدِ العمل.

تنصُّ قواعدُ البياناتِ المحليَّةِ أنَّ البياناتِ يجبُ أن تكونَ مخزَّنةً ومحفوظةً في الدولةِ الَّتي حُصِلَ عليها منها ، و قد يبدو ذلك ضدَّ منطقِ المجتمعِ الرقميّ الحديثَ الَّذي لا حدود له ، ولكنَّ هذه السيطرةَ هي إمَّا متطلَّبٌ مباشرٌ أو نتيجةٌ فرعيَّةٌ للعديدِ من قوانينِ حمايةِ البياناتِ الجديدة .

تتطلَّبُ المخاطرُ الناشئةُ من استراتيجيَّةِ عملٍ عابرةٍ للحدودِ نهجاً جديداً في تطويرِ واقتناءِ خدماتِ الحوسبةِ السحابيَّةِ في جميعِ نماذجِ الخدمةِ ، و يتعاملُ المسؤولونَ عن إدارةِ الأمانِ والمخاطرِ مع منظر قانونيّ غيرِ متجانسٍ إذ يتطلَّبُ كلُّ مجالٍ معيَّنٍ في حماية البياناتِ استراتيجيَّاتٍ خاصَّةً قد لا تكون مناسبةً لاستخدامها في مجالاتٍ أخرى ، وبالتالي يصبحُ تخطيطُ مكانِ تخزينِ البياناتِ أحدَ أولويَّاتِ تطويرِ واقتناءِ خدماتِ الحوسبةِ السحابيَّة .

أصبحَتْ معالجةُ البياناتِ في البيئاتِ غيرِ الموثوقةِ - مثلَ سحابةٍ عامَّةٍ - ومشاركةُ البياناتِ والتحليلاتِ بينَ عدّةِ أطرافٍ ضروريَّةٍ لنجاحِ الشركاتِ ، و يجعلُ التعقيدَ المتزايدَ لمحركاتِ التحليلِ والبنى التحتيَّةِ ضروريَّاً لأن يدمجَ مزوّدو الخدماتِ وظيفةَ الخصوصيَّةِ منذُ البدايةِ ، و انتشار نماذجِ الذكاءِ الاصطناعيّ وضرورةِ تدريبِها هو مجرَّدَ إضافةٍ حديثةٍ لمخاوفِ الخصوصيَّة .

على عكسِ الضوابطِ الأمنيَّةِ العاديَّةِ للبياناتِ في حالةِ الراحةِ ، و تحمي معالجةُ البياناتِ الوديَّةِ للخصوصيَّةِ (PEC) البياناتِ في أثناءِ الاستخدام ، ونتيجةً لذلك يمكنُ للشركاتِ إجراءُ معالجاتِ البياناتِ والتحليلاتِ الَّتي كانَتْ غيرَ ممكنةٍ في الماضي بسببِ مخاوفِ الخصوصيَّةِ أو الأمان .

تتوقَّعُ شركةُ Gartner أنَّ 60٪ من الشركاتِ الكبيرةِ ستستخدمُ تقنيَّات PEC على الأقلّ في مجالاتِ التحليلِ وذكاءِ الأعمالِ ، أو الحوسبة السحابيَّةِ بحلولِ عامِ 2025م .

و سيؤدّي الطلبُ المتزايدُ من المستهلكينَ على حقوقِ المتضرّرينَ وتزايدِ التوقّعات بالشفافيَّة إلى زيادةِ الحاجةِ إلى تجربةِ استخدامٍ مركزيَّةٍ لحمايةِ البيانات (Privacy User Experience)

لقد أدركّتْ الشركاتُ المتطلَّباتُ المستقبليَّةُ المتعلّقةِ بدمجِ جميعِ جوانبِ تجربةِ مستخدمِ حمايةِ البياناتِ – تعليمات ، ملفاتُ تعريفِ الارتباطِ ، و إدارةِ الموافقاتِ ومعالجةِ طلباتِ حقوقِ المتضرّرينَ - في بوابةِ الخدمةِ الذاتيَّة ، و يوفّرُ هذا النهجُ الراحةَ لأطرافِ العملِ الرئيسيَّة (العملاء والموظفين) ، ويؤدّي إلى توفيرِ وقتٍ وتكاليفَ كبيرة .

تتوقَّعُ شركةُ Gartner أنَّ 30٪ من الشركاتِ التي تتعاملُ مع العملاءِ ستقدّمُ بوَّابةَ شفافيةِ خدمةٍ ذاتيَّةٍ لإدارةِ التفضيلاتِ والموافقاتِ خلالَ الأعوامِ القادمة.

وفي النهايةِ أريدُ أن أضيفَ أنَّه مع التحوّلِ إلى نماذجِ عملٍ وحياةٍ متشابكةٍ ، و تزدادُ كلٌّ من إمكانيةِ ورغبةِ زيادةِ التتبعِ والمراقبةِ وغيرها من الأنشطةِ المتعلّقةِ بمعالجةِ البياناتِ الشخصيَّةِ ، وتتصاعدُ مخاوفُ حمايةِ الخصوصيَّة إلى المقدمة .

ونظراً لتأثيرِ النظامِ المتشابكِ للتفاعلاتِ على الخصوصيَّة ، زادّتْ أيضاً منتجيَّة ورضا التوازنِ بينَ العملِ والحياةِ في مختلفِ الصناعاتِ والتخصّصاتِ ، إذ يجبُ على الشركاتِ اتّباعُ نهجٍ متمركزٍ حولَ الإنسانِ

فيما يتعلَّقُ بحمايةِ البياناتِ ، ويجبُ استخدامُ بياناتِ المراقبةِ فقط بشكلٍ محدودٍ ولأغراضٍ واضحةٍ ، مثلَ تحسينِ تجربةِ الموظَّفِ من خلالِ إزالةِ التوتّرِ غيرِ الضروريّ ، أو تقليلِ مخاطرِ الاحتراقِ عن طريقِ كشفِ مخاطرِ الإجهاد ..

حماية البيانات في قطاع الرعاية الصحية

تلعبُ حمايةُ البياناتِ دوراً حاسماً في قطّاعِ الرعايةِ الصحيَّةِ ، حيثُ تُعَالجُ معلوماتٌ حسَّاسةٌ وشخصيَّةٌ عن المرضى وحالتِهم الصحيَّةِ ، و حماية هذه البياناتِ الحسَّاسةِ أمرٌ بالغَ الأهميَّة للحفاظِ على خصوصيَّةِ المرضى وبناءِ الثقةِ وضمانِ سلامةِ نظامِ الرعايةِ الصحيَّة .

تتعلَّقُ حمايةُ البياناتِ في قطَّاعِ الرعايةِ الصحيَّةِ بالتدابيرِ القانونيَّةِ والتقنيَّةِ والتنظيميَّةِ الَّتي تُتَّخذُ لحمايةِ البياناتِ الشخصيَّةِ الصحيَّةِ من الوصولِ غيرِ المصرَّحِ به ، والاستخدام غيرِ المشروعِ ، والفقدانَ أو السرقة ، و تعدُّ قوانينُ حمايةِ البياناتِ الوطنيَّةِ واللَّوائح الخاصَّة مثلَ اللَّائحةِ العامَّةِ لحمايةِ البياناتِ ذاتِ الصلة في أوروبا.

إنَّ أحدَ أهمّ المبادئِ في حمايةِ البياناتِ في قطَّاعِ الرعايةِ الصحيَّةِ هو سريَّةُ البيانات و يعني ذلك أنَّهُ يجبُ أنْ يكونَ للأشخاصِ المصرَّحِ لهم فقط القدرةَ على الاطّلاعِ على البياناتِ الشخصيَّةِ الصحيَّةِ ومعالجتها ، إذ يجبُ اتّخاذُ التدابيرِ التقنيَّةِ والتنظيميَّةِ المناسبةِ لتقييدِ الوصولِ إلى هذهِ البياناتِ الحسَّاسةِ وضمانِ سرّيتها .

مبدأ آخرٌ أساسيٌّ هو سلامةُ البياناتِ ، إذ يجبُ أن تكونَ البياناتُ صحيحةً وكاملةً وحديثة ، و يجب منعُ التلاعبِ أو التغييرِ غيرِ المصرَّحِ به للبياناتِ الصحيَّةِ لضمانِ استنادِ القراراتِ الطبيَّةِ إلى معلوماتٍ موثوقة .

بالإضافةِ إلى السريَّةِ والسلامةِ ، يلعبُ توفّرُ البياناتِ أيضاً دوراً مهمَّاً، و يحتاجُ الفريقُ الطبيُّ إلى الوصولِ إلى معلوماتٍ صحيَّةٍ ذاتِ الصلة في أيّ وقتٍ من الأوقاتِ لتقديمِ العلاجِ والرعايةِ المناسبةِ ، لذا يجبُ تخزينُ البياناتِ بشكلٍ آمنٍ وتوفيرُ الوصولِ إليها ، في الوقتِ ذاتِه حمايتُها من الوصولِ غير المصرَّحِ به.

تتطلَّبُ حمايةُ البياناتِ في قطَّاعِ الرعايةِ الصحيَّةِ أيضاً تدريباً شاملاً للموظَّفينَ وزيادةَ الوعي لديهم ، لضمانِ فهمِهم لقواعدِ حمايةِ البياناتِ وتطبيقِها بشكلٍ صحيحٍ ، إذ يجبُ تطويرُ سياساتٍ وإجراءاتٍ واضحةٍ لضمانِ التعاملِ الآمنِ مع البياناتِ الصحيَّةِ ومنعَ انتهاكاتِ حمايةِ البيانات .

في النهايةِ، تهدفُ حمايةُ البياناتِ في قطَّاعِ الرعايةِ الصحيَّةِ إلى حمايةِ خصوصيَّةِ وكرامةِ المرضى من خلالِ ضمانِ اتّخاذِ التدابيرِ المناسبةِ لحمايةِ البياناتِ الصحيَّةِ الحسَّاسة ، و يمكنُ للمرضى أن يثقوا بأنَّ بياناتِهم الشخصيَّةَ الحسَّاسة في أيدي آمنةٍ وأنَّ خصوصيَّتهم ستُحتَرم في الوقتِ نفسه ، تساهمُ حمايةُ البياناتِ في الحفاظِ على سلامةِ نظامِ الرعايةِ الصحيَّةِ وتحسينِ جودةِ الرعايةِ الطبيَّة .

السرُّ الطبيُّ للأطبَّاءِ هو التزامٌ قانونيٌّ يحمي سريَّةَ المعلوماتِ الطبيَّةِ وخصوصيَّةَ المرضى ، إذ إنَّه جزءٌ أساسيٌّ من الأخلاقِ الطبيَّةِ ويستندُ إلى مبدأ الثقةِ بينَ الطبيبِ والمريضِ .

يُلزَمُ الأطبَّاءُ بالسرَ المهنيّ للحفاظِ على سريَّةِ جميعِ المعلوماتِ الَّتي يُكشَفُ عنها لهم أو يتعلَّمونها في أثناءِ ممارستِهم الطبيَّة ، يشملُ ذلك التشخيصاتِ الطبيَّةَ وسجلَّاتِ العلاجِ والأوضاعَ الشخصيَّة وغيرها من المعلوماتِ السريَّةِ الَّتي يُكشَفُ عنها أو الحصول عليها في أثناءِ علاقةِ الطبيبِ والمريض .

والأطبَّاءُ ملزمونَ قانونيَّاً بالامتثالِ للسرّ المهنيّ ، و يوفّرُ هذا التزاماً في مختلفِ القوانينِ الوطنيَّةِ والمبادئِ الأخلاقيَّة ، مثلَ قانونِ العقوباتِ الألمانيّ (§ 203 StGB) أو مبادئِ المهنةِ الطبيَّة.

يهدفُ السرُّ المهنيّ إلى تعزيزِ ثقةِ المرضى في الطبيبِ والنظامِ الصحي ، إذ يتيحُ للمرضى التحدُّثَ بصراحةٍ وصدقٍ حولَ مشاكلِهم الصحيَّة بدونِ الخوفِ من انتهاكِ خصوصيَّاتِهم أو الكشفِ عن معلوماتِهم الحسَّاسة .

ومع ذلكَ ، هناكَ استثناءاتٌ يمكنُ فيها تخلي الأطبَّاءِ عن سرية المعلومات ، مثل عندما يُعطي المريضُ موافقتَه على الكشفِ عن المعلوماتِ أو عندَ وجودِ التزامٍ قانوني ، مثلَ تقاريرِ بعضِ الأمراضِ المعدية.

ينطبقُ السرُّ المهنيّ أيضاً على العاملين الآخرين في المهن الطبيَّةِ ، مثل الممرضاتِ والأخصَّائيين العلاجيّين والموظَّفينَ الطبّيين الَّذينَ يحصلونَ على وصولٍ إلى بياناتِ المرضى السريَّةِ في أثناءِ ممارسةِ عملهم .

يمكنُ أن يكونَ انتهاكُ السرّ المهنيّ للأطباءِ له عواقبَ جنائيَّة وعواقب أخلاقية ، بما في ذلكَ

التدابيرَ الانضباطيَّة أو **فقدانَ الترخيص الطبي .**

بشكلٍ عامٍ ، يضمنُ السرُّ المهنيُّ للأطباءِ حمايةَ خصوصيَّةِ وسريَّةِ المعلوماتِ الطبيَّةِ للمرضى ، ويعدُّ جزءاً أساسيَّاً من الأخلاقِ الطبيَّة.

تنظمُ المادَّة 203 من قانونِ العقوباتِ في ألمانيا (StGB) السرَّ المهنيَّ لممارسي المهنِ الصحيَّةِ ، وخاصَّةً الأطبَّاء وأطبَّاء الأسنانِ والأخصَّائيّين النفسيّين السلوكيّين وأطبَّاءَ العلاجِ النفسيّ للأطفالِ والمراهقين ، وكذلكَ الصيادلة .

تنصُّ المادَّة /203/ من قانونِ العقوباتِ على أنَّه يتعيَّن على هذه المجموعاتَ المهنيَّةِ الحفاظُ على السريَّة بشأنِ "سرّ ثقةٍ كُلِفوا أو أصبحَ معروفاً لديهم في صفتِهم كممارسينَ لمهنةٍ صحيَّةٍ " ، وهذا يعني أنَّه يجبُ عليهم عدمُ الكشفِ عن المعلوماتِ السريّةِ الَّتي يحصلونَ عليها في إطارِ عملِهم المهنيّ من دونِ موافقةِ المريض .

و بموجبِ المادَّةِ /203 / من قانونِ العقوباتِ ، تُغطَّى المعلوماتُ التي يُكلَّفُ ممارسُ المهنةِ بها أو أصبَحَتْ معروفةً لديه في إطارِ ممارستِه المهنيَّةِ ، و يمكنُ أن تشملَ هذه التشخيصاتُ الطبيَّةُ تطوّرات العلاجِ والظروفَ الشخصيَّةَ وغيرها من المعلوماتِ الحسَّاسةِ الَّتي تُكشَفُ في أثناء العلاجِ أو الاستشارةِ.

و من المهم ملاحظةُ أنَّ السرَّ المهنيَّ وفقاً للمادة /203/ من قانونِ العقوباتِ يمثّلُ التزاماً جنائياً ، و في حالةِ انتهاكِ هذا الالتزامِ ، يواجهُ ممارسو المهنةِ عقوباتٍ قانونيَّةً ، وخاصَّةً عقوباتٍ ماليَّةً أو عقوباتِ حبسٍ تصلُ إلى عامٍ واحد ، و في الحالات الخطيرة ، يمكنُ أن تكونَ العقوبةُ أعلى .

ومع ذلكَ ، فهناك بعضُ الاستثناءاتِ الَّتي يمكنُ أنْ تتسبَّبَ في انتهاكِ السرّ المهنيّ ، على سبيلِ المثالِ ، توجدُ استثناءاتٌ عندما يعطي المريضُ موافقتَه صراحةً على الكشفِ عن المعلوماتِ ، و أيضاً في حالةِ التزامٍ قانوني بالكشفِ عن المعلوماتِ ، مثلَ حالةِ وجودِ مرضٍ معدٍ قابلٍ للإبلاغ ، يمكن أن يكونَ السرُّ المهني محدودًا.

و يهدفُ السرُّ المهنيُّ إلى تعزيزِ الثقةِ بين ممارسي المهنِ الصحيَّةِ ومرضاهم وحمايةِ خصوصيَّة معلوماتِ المرض ، يتيحُ للمرضى التعبيرَ بصراحةٍ وصدقٍ والشعورَ بالأمانِ بأنَّ معلوماتهم الحسَّاسةَ بيدِ خبراءَ موثوقين .

و بشكلٍ عام ، تضمنُ المادَّةُ /203/ من قانونِ العقوباتِ أنَّ ممارسي المهنِ الصحيَّة يلتزمونَ بواجبِ السريَّةِ المهنيَّة وحمايةَ سريَّةِ معلوماتِ المرضى ، وبالتالي تُعزَّزُ ثقةُ المرضى ويضمنُ النزاهةَ في الرعايةِ الصحيَّة والامتثال للمعاييرِ الأخلاقيَّة .

المادة 34 من قانون العقوبات (StGB) في ألمانيا تنصُّ على وجودِ عمليَّة ضروريَّة مبرَّرة ، و تنظّمُ هذه المادَّةُ تبريرَ ارتكابِ فعلٍ إجرامي عندما يكونُ ضرورياً للدفاعِ عن هجومٍ غيرِ قانوني و معاصر على النفسِ أو على شخصٍ آخر.

تنصُّ المادَّةُ على أنَّ الشخصَ الَّذي يرتكبُ جريمةً لا يُعَاقبُ إذا كانَتْ هذه الجريمةُ تجري لحمايةِ مصلحةٍ قانونيَّةٍ للنفسِ أو للآخرين ، شريطةَ توفّرِ الشروطِ التالية :

1- حالة الضرورة : يجبُ أن يكونَ هناكَ خطرٌ قائمٌ وغيرُ قانوني ، أي إجراءٌ غيرُ قانونيّ قائمٍ أو بدأ بالفعلِ يهدّدُ الحياةَ أو الجسمَ أو الحريَّةَ أو الملكيَّةَ أو حقوق قانونيَّة أخرى هامة .

2- الضرورة : يجبُ أن تكونَ الفعلةُ القاضيةُ بردّ الهجومِ ضروريَّةً ، وهذا يعني أنَّه لا تتوفّر وسائلُ أكثرَ خفَّةً لصدّ الهجومِ ، و يُبرَّرُ انتهاكُ حقوقِ الخصوصيَّةِ من أجلِ الدفاعِ عن هذا الهجوم .

3- توازن المصالح : يجب أن يُجرى توازنٌ بينَ المصالحِ المتعارضةِ ، يُقارنُ الحقُّ القانونيُّ المحميُ الَّذي يجبُ حمايُته من خلالِ انتهاكِ حقوقِ الخصوصيَّةِ مع الحقّ القانونيّ المحميّ الَّذي يتعرَّضُ للتهديدِ من خلالِ الفعلِ ، و يجب أن تكونَ مبرّراتُ انتهاكِ حقوقِ الخصوصيَّةِ أكثرَ أهميَّةً من الانتهاكِ ذاتِه للخصوصيَّة .

و من المهمّ أن نلاحظَ أنَّ الضرورةَ المبرّرةَ في سياقِ حمايةِ البياناتِ هي استثناءٌ ، ويمكنُ تطبيقُها فقط في حالاتٍ معيَّنة ، يتطلَّبُ تطبيقُ هذه المادَّة مراجعةً دقيقةً للظروفِ الفرديَّةِ وتوازنُ الحقوقَ المعنيَّة .

وفقًا للمادة /138/ من قانونِ العقوباتِ الألماني (StGB) يُعتبر عدمُ الإبلاغِ عن جرائمَ مخطَّط لها أمراً محظوراً .

تنصُّ هذه المادَّةُ على أن الشخص الَّذي يتلَّقى معلوماتٍ حولَ جريمةٍ خطيرةٍ مخطَّط لها والَّتي تهدّد الحياة أو السلامة الجسديَّةَ أو الحريَّةَ الشخصيَّةَ أو الحيازةَ بقيمةٍ كبيرةٍ ، مُلزَمٌ بالإبلاغِ عن ذلكَ إلى السلطاتِ القضائيَّة ، ما لم ينطبق استثناءٌ ما .

يهدف القسم /138/ من قانونِ العقوباتِ إلى تعزيزِ منعِ الجرائمِ الخطيرةِ المخطَّطِ لها في الوقت المناسب وضمانِ الأمنِ العام ، و يحدّدُ هذه المادَّة الواجب على الأشخاصِ الَّذينَ يتلّقون معلوماتٍ عن تخطيطِ جرائمٍ من هذا النوعِ أن يبلّغوا السلطاتِ المختصَّة ، وذلك لتمكينِ إجراءاتِ العدالةِ الجنائيَّةِ الفعَّالة .

و من المهمّ أن نلاحظَ أنَّ عدمَ الإبلاغِ عن جريمةٍ مخطَّطٍ لها يُعتبَرُ جرماً في ظروفٍ معيَّنةٍ ، و إذا كانَتْ الجريمةُ المخطَّطُ لها تُشكّلُ تهديداً للحياةِ أو السلامةِ الجسديَّةِ أو الحريَّةِ الشخصيَّةِ أو الحيازةِ بقيمةٍ كبيرةٍ ، فإنَّ عدمَ الإبلاغِ عن هذه الجريمةِ يُعتبَرُ جريمةً ، ما لم ينطبق استثناءٌ ما .

ومع ذلكَ ، هناكَ أيضاً استثناءاتٌ من الواجبِ الإبلاغُ بموجبِ القسم /138/ من قانونِ العقوبات ، على سبيلِ المثالِ ، ليسَ من واجبِ أقرباءِ الدم مثلَ الزوجين أو الشركاءِ أو أفرادِ العائلةِ في الخطّ المستقيمِ القرابة أن يبلّغوا عن جريمةٍ مخطَّطٍ لها ، ما لم تكُن تلكَ الجرائم من بينِ الجرائمِ الخطيرةِ مثلَ القتلِ أو القتلِ العمد .

و يكمنُ الهدفُ من هذا القسمِ الجزائيّ في تعزيزِ تعاونِ الجمهورِ مع السلطاتِ القضائيَّةِ ودعمِ جهودِ مكافحةِ الجرائمِ الخطيرةِ بشكلٍ فعَّالٍ ، و يمكنُ أن يسهمَ الإبلاغُ عن جرائمٍ مخطَّطٍ لها في منعِ الجرائمِ في وقتٍ مبكّر ومساءلةِ الجناة .

من المهمّ أن نلتزمَ بالأحكامِ القانونيَّةِ الدقيقةِ للقسم /138/ من قانونِ العقوباتِ ، حيثُ يمكنُ أن تختلفَ هذه الأحكامُ حسبَ الحالةِ والنظامِ القانوني .

هنا سأقومُ بشرحِ الفقراتِ المذكورةِ بشكلٍ مفصَّلٍ لكلّ فقرةٍ من المادةِ /139/ من قانونِ العقوباتِ الألماني

(1)وفقًا للمادَّةِ /138/ من قانونِ العقوباتِ الألماني (StGB) ، يتعلَّقُ الأمرُ بمحاولةِ ارتكابِ جريمةٍ ، إذا لم تتمُّ محاولةُ الجريمةِ ، فهذا يعني أنَّ المتَّهمَ لم يبدأ نشاطاً فعليّاً لارتكابِ الجريمةِ ، في مثلِ هذه الحالاتِ، يمكنُ التنازلُ عن فرضِ عقوبةٍ ، وهذا يعني أنَّ المتَّهمَ لا يعاقَبُ على محاولةِ الجريمةِ ، وإنَّما يُعاقَبُ فقط إذا ارتُكِبَت الجريمةُ بشكلٍ كامل .

(2)تنصُّ الفقرةُ على أنَّ الأشخاصَ الروحيّينَ ، بما في ذلكَ أولئكَ الَّذينَ يعملونَ كمعالجينَ روحيّين ، غير ملزمينَ بالإبلاغِ عما أُسندَ إليهم في إطارِ دورِهم كمعالجينَ روحيّينَ ، وهذا يعني أنَّهُم مُسمَّونَ لحفظِ السريَّةِ حولَ المعلوماتِ الَّتي أُسنِدت إليهم في سياقِ الرعايَة الروحيَّة، ولا يلزمهم الكشفُ عن هذهِ المعلوماتِ للسلطاتِ القضائيَّةِ .

(3)في هذهِ الفقرةِ ، يتعلَّقُ الأمرُ بالامتناعِ عن تقديمِ بلاغٍ ضدَّ أحدِ الأقاربِ ، إذا ارتكبَ شخصٌ ما جريمةً وتحمَّلَ شخصٌ آخرٌ معرفةً بذلك وكانَ مطالباً بتقديمِ بلاغٍ ، ولكنَّهُ تغاضَى عن ذلك ، فقد يظلُّ غيرَ مُعَاقَب، إذا بذلَ جهوداً جادَّةً لمنعِ القريبِ من ارتكابِ الجريمةِ أو لمنعِ نجاحِها ، ولكنَّ هناكَ بعضَ الجرائمِ الخطيرةِ ، مثلُ القتلِ أو القتلِ العمدِ ، و الإبادةِ الجماعيَّةِ، و الجرائمَ ضدَّ الإنسانيَّة ، جرائم الحرب ،

و الخطفُ مع التهديدِ بالقتلِ ، و احتجازِ الرهائنِ أو الاعتداءِ على النقلِ الجويّ والبحريَ من قبلِ جماعةٍ إرهابيَّةٍ ، و لا ينطبقُ فيها هذا الاستثناء ، وهذا يعني أنَّهُ في مثلِ هذهِ الحالاتِ ، لن يظلَّ الامتناعُ عن تقديمِ البلاغِ من دونِ عقاب .

وبالإضافةِ إلى ذلك ، تنصُّ هذه الفقرةُ أنَّ المحامينَ والمدافعينَ والأطبَّاءَ والأخصَّائيّين النفسيّينَ والمعالجينَ النفسيّين السريريّينَ والمعالجينَ النفسيّينَ للأطفالِ والمراهقينَ غير مُلزمينَ بالإبلاغِ عن

المعلوماتِ الَّتي أُسنِدّتْ إليهم في هذهِ الوظيفة ، والشروطَ نفسِها تنطبقُ على المساعدينَ المهنيّينَ لهؤلاءِ الأشخاصِ المذكورينَ والأشخاصِ الَّذينَ يعملونَ تحتَ إشرافِهم تحضيراً للمهنةِ ، هؤلاءِ الأشخاص مسموحٌ لهم بإبقاءِ المعلوماتِ الَّتي أُصبحَتْ معروفةً لديهم في إطارِ وظيفتِهم سريَّةً وليسَ عليهِم الإفصاحُ عنها للسلطاتِ القضائيَّة .

(3)هذه الفقرةُ تتعلَّقُ بالإفلاتِ من العقابِ للشخصِ الَّذي يحاولُ تنفيذَ الجريمةِ أو نجاحها بطرائقَ أخرى غيرِ الإبلاغِ عنها ، و إذا تدخَّلَ الشخصُ ومنعَ تنفيذَ الجريمةِ أو نجاحَها من دونِ تقديمِ بلاغٍ ، فسيظلُّ غيرَ معاقبٍ ، و إذا لم تُنفَّذ الجريمةُ أو نجحَتْ من دونِ تدخّلِ الشخصِ المُلزَمِ بالإبلاغِ ، فإنَّ السعيَ الجديَّ من جانبه لمنعِ نجاحِ الجريمةِ يكفي لإعفائِه من العقاب .

هذه الفقراتُ تنظّمُ بعضَ الاستثناءاتِ في القانونِ الجنائيّ الألمانيّ وتضمنُ أنَّ بعضَ المهنِ ، مثلَ مهنةِ رجالِ الدّينِ والمحامينَ والأطبَّاءَ والمعالجينَ النفسيّينَ ، لديهم حقوقُ الحفاظِ على السريَّةِ المهنيَّةِ وعدمُ الإفصاحِ عن المعلوماتِ الَّتي يُكشَفُ عنها لهم في إطارِ وظائفِهم المهنيَّة .

تتعلَّقُ الموازنةُ بينَ المادّة /203/ والمادَّة /34 / من قانونِ العقوباتِ الألمانيّ بالتوازنِ بينَ سريَّةِ المعلوماتِ الطبيَّةِ وواجبِ الإبلاغِ عن جرائم ، فوفقاً للمادة /203/ من قانونِ العقوباتِ الألمانيّ ، يُلزِمُ الأطبَّاءُ وحاملو السرّ المهنيّ الآخرونَ بالصمتِ بشأنِ جميعِ الأسرارِ الَّتي كُلِّفوا بها في ممارستِهم المهنيَّة. و يهدفُ هذا السرُّ إلى حمايةِ الخصوصيةِ وبناءِ الثقةِ بين الطبيبِ والمريضِ ، و لا يجوزُ للأطبَّاءِ الكشفُ عن المعلوماتِ السريَّةِ من دونِ موافقةِ المريضِ ، ما لم تكُنْ هناك استثناءاتٌ قانونيَّة .

و من ناحيةٍ أخرى ، هناكَ المادَّة /34/ من قانونِ العقوباتِ الَّتي تنصُّ على واجبِ الإبلاغِ عن الجرائم وفقاً لهذا البندِ ، و لا تُلزَمُ بعضُ الفئاتِ المهنيَّة مثلَ الأطبَّاءِ والمحامينِ وأخصائيّ العلاجِ النفسيّ إلخ بالإبلاغِ عن الجرائمِ الَّتي يكتشفونَها في ممارستِهم المهنيَّةِ ، ما لم يكونوا قد بذلوا جهوداً جادَّةً لمنعِ الجاني من ارتكابِ الجريمةِ أو لمنعِ وقوعِها .

تتضمَّنُ الموازنةُ بين المادتين /203/ و /34/ من قانونِ العقوباتِ موازنةً بينَ المصالحِ المتعارضةِ لحمايةِ خصوصيَّةِ المريضِ وضمانِ الأمنِ العام ، و من جهةٍ هناكَ سريَّةُ المعلوماتِ الطبيَّةِ الَّتي تضمنُ سريَّةَ المعلوماتِ الشخصيَّة وحمايةَ المريضِ ، ومن جهةٍ أخرى هناكَ الالتزامُ بالإبلاغِ عن الجرائمِ لضمانِ الأمنِ العام ومحاسبةِ الجُناةِ المحتمَلين .

و عندَ إجراءِ الموازنةِ بين المادتين /203/ و /34/ من قانونِ العقوباتِ ، يجبُ مراعاةُ عدّةِ عواملَ مثلِ نوعِ وخطورةِ الجريمة ، واحتمالِ وقوعِ أضرارٍ إضافيَّةٍ ، والعلاقةُ بينَ الطبيبِ والمريضِ ، بالإضافةِ إلى الأحكامِ القانونيَّةِ والاستثناءاتِ المنصوصِ عليها في القوانينِ المعمولِ بها.

و بشكلٍ عام ، تعدُّ سريَّةُ المعلوماتِ الطبيَّةِ قيمةً عاليةً ويجبُ اختراقُها فقط في حالاتٍ استثنائيَّةٍ عندما يكونُ للمصلحةِ العامَّةِ أو لمصلحةِ المريضِ أفضليَّةٌ في الكشفِ عن الجريمةِ ،و يقعُ على عاتقِ الطبيبِ أنْ

يقومَ بتوازنٍ مناسبٍ بينَ هذه المصالحِ والحصولِ على المشورةِ القانونيَّةِ إذا لزمَ الأمرُ لاتّخاذِ القرارِ الصحيح .

تتعلَّقُ الموازنةُ بين المادَّتين /138/ و/139/ من قانونِ العقوباتِ الألمانيّ بالتوازنِ بينَ جريمةِ عدمِ الإبلاغِ عن الجرائمِ المخطَّطِ لها وحمايةِ سريَّةِ المهنة .

و وفقاً للمادَّةِ /138/ من قانونِ العقوباتِ الألمانيّ ، يعدُّ عدمُ الإبلاغِ عن الجرائمِ المخطَّطِ لها ، وخاصَّةً تلك الَّتي تستهدفُ الحياةَ أو السلامةَ الجسديَّة أو الحريَّةِ الجنسيَّة جريمةً يعاقبُ عليها القانونُ ، و تهدفُ هذه المادَّةُ إلى ضمانِ الأمنِ العام وحمايةِ المحتملينَ من الجرائمِ ، و تنصُّ المادَّةُ على وجوبِ الإبلاغِ العام عن الجرائمِ المخطَّطِ لها .

و من ناحيةٍ أخرى ، هناكَ المادَةُ /139/ من قانونِ العقوباتِ الَّتي تنظّمُ سريَّةَ المهنة ، فوفقاً لهذه المادَّة، يجبُ على بعضِ المهنِ مثلَ الأطبَّاءِ والمحامينَ وأخصائيّ العلاجِ النفسيّ وغيرِهم من حاملي السرّ المهنيّ الآخرينَ الحفاظُ على سريَّةِ المعلوماتِ الَّتي يحصلونَ عليها في ممارسةِ مهنتِهم ، و يستندُ هذا الالتزامُ إلى علاقةِ الثقةِ بينَ حاملِ السرّ المهنيّ والشخصِ الَّذي يكلّفُه بالمعلومات ، و تعد سريَّةُ المهنةِ قيمةً هامَّةً تضمنُ حمايةَ الخصوصيَّةِ وسريَّةَ التواصل .

و عندَ الموازنةِ بين المادَّتين /138/ و /139/ من قانونِ العقوباتِ ، إذ يجبُ مراعاةُ عدَّةِ عوامل ، و تشملُ هذه العواملُ خطورةَ الجريمةِ المخطَّطِ لها ، والمخاطرَ الَّتي يتعرَّضُ لها المجرمونَ المحتمَلون ، والعلاقةَ بين حاملِ السرّ المهنيّ والشخصِ الَّذي كلَّفهُ بالمعلومات ، بالإضافةِ إلى الاستثناءاتِ والقيودِ المنصوصِ عليها في القوانينِ المعمولِ بها .

و بشكلٍ عام ، يعدُّ الإبلاغُ عن الجرائمِ المخطَّطِ لها وفقاً للمادَّة /138/ من قانونِ العقوباتِ أولويَّةً على سريَّةِ المهنةِ وفقاً للمادَّةِ /139/ من القانونِ ، وهذا يعني أنَّ حاملي السرّ المهنيّ ، بما في ذلك الأطبَّاء، مُلزَمونَ في بعضِ الحالاتِ بالإبلاغِ عن الجرائمِ المخطَّطِ لها ، حتَّى لو تعارضَ ذلك مع سريَّةِ مهنتهم . ويمكنُ أنْ تختلفَ الشروطُ والاستثناءاتُ المحدَّدةُ حسبَ النظامِ القانونيّ والظروفِ المحدَّدة .

و من المهمّ ملاحظةُ أنَّ الموازنَةَ الدقيقةَ بين المادَّتين /138/ و /139/ من قانونِ العقوباتِ تعتمدُ على عواملَ متعدّدةٍ وأنَّ الأحكامَ القانونيَّةَ وتفسيرها قد تختلفُ من حالةٍ إلى أخرى .

وفقاً للمادَّة /202/ من قانونِ العقوباتِ الألمانيّ(StGB) ، يُعدُّ انتهاكُ السريَّةِ البريديَّةِ جريمةً قابلةً للمسائلةِ ، و تهدفُ هذه البنودُ إلى حمايةِ حقّ الخصوصيَّةِ والسريَّةِ في التواصل ، وخاصَّةً فيما يتعلَّقُ بالرسائلِ البريديَّةِ ، والتلغراف ، والبريد الإلكترونيّ ، وغيرِها من الرسائلِ الكتابيَّة .

و تشملُ جريمةُ انتهاكِ السريَّةِ البريديَّةِ الوصولَ غيرَ المخوَّلَ إلى أو المعرفةِ السريَّةِ لرسائلِ الآخرينَ ، وتشملُ فتحَ الرسائلِ ، وقراءتَها ، ونسخَها ، واعتراضَها ، واستنطَاقَها، أو أيَّ أفعالٍ غيرِ مخوَّلةٍ تنتهكُ سريَّةَ التواصل .

و إنَ التجريمَ المتعلّقَ بانتهاكِ السريَّةِ البريديَّةِ لا ينحصرُ فقط في الرسائلِ الورقيَّةِ ، بل يمتدُّ أيضاً إلى وسائلِ التواصلِ الحديثةِ مثلَ البريدِ الإلكترونيّ والرسائلِ النصيَّةِ ووسائلِ التواصلِ الاجتماعي ،و يتمتَّعُ الشخصُ بحقّ حمايةِ خصوصيَّته وسريَّةِ تواصلهِ في جميعِ أشكالِ المراسلاتِ الكتابيَّةِ والإلكترونية .

و تنصُّ المادَّةُ /202/ من قانونِ العقوباتِ الألمانيّ على أنَّ جريمةَ انتهاكِ السريَّةِ البريديَّةِ تعاقبُ بالسجنِ حتَّى عامٍ واحدٍ أو بغرامةٍ ماليَّة ، وفي الحالاتِ الخطيرة ، مثلَ جرائمِ الانتهاكِ المنظَّمِ أو استخدامِ المعلوماتِ المكتسبةِ للابتزازِ أو الغش ، يمكنُ أنْ يكونَ العقابُ أشد .

و من المهمِ الإشارةُ إلى أنَّ السريَّةَ البريديَّةَ هي حقٌّ أساسيٌّ وتضمنُ حمايةَ الخصوصيَّةِ والبياناتِ الشخصيَّةَ في مجتمعٍ حديثٍ ، ولذلك تتمُّ متابعةُ ومعاقبةُ أيّ انتهاكٍ لهذا الحقّ بحزمٍ ، من أجلِ حمايةِ سريَّةِ التواصلِ وحقوقِ الأفرادِ الشخصيَّة .

بموجبِ القانونِ الجنائيّ الألماني(StGB) الفصلُ 202 الفقرة الأولى ، يُعد "التجسّس على البياناتِ " جريمةً تهدفُ إلى حمايةِ البياناتِ والخصوصيَّةِ الشخصيَّة .

و تتمثّلُ الجريمةُ في الحصولِ على البياناتِ من دونِ إذنِ صاحبِ الحقّ و من دونِ تصريحٍ للمعلوماتِ غيرِ المخصَّصةِ للشخصِ الَّذي يحصلُ عليها ، والَّتي تكونُ محميَّةً من الوصولِ غيرِ المصرَّحِ به ، و قد تكونُ هذه البياناتُ مخزَّنَةً في نظامٍ إلكترونيّ مثلَ جهازِ كمبيوتر أو هاتفٍ ذكيّ أو شبكة ، كما يشملُ هذا الجرمُ الاستماعَ أو اعتراضَ الاتّصالاتِ الإلكترونيَّةِ مثلَ البريدِ الإلكترونيّ أو رسائلِ الدردشة .

تتضمَّنُ الجريمةُ أيضاً اختراقَ أنظمةِ الكمبيوترِ الأجنبيَّةِ من دونِ إذنٍ للحصولِ على البياناتِ ، كما يُعتبَرُ غيرُ مشروعٍ أن يحصلَ الشخصُ على وصولٍ للبياناتِ الَّتي ليسَ لهُ الحقُّ فيها بوساطةِ التقنيَّةِ ، مثلَ اختراقِ كلماتِ المرورِ أو تجاوزِ تدابيرِ الأمان .

ينصُّ القانونُ على عقوبةِ حبسٍ تصلُ إلى ثلاثِ سنواتٍ أو غرامةٍ ماليَّةٍ للتجسّس على البياناتِ ، في الحالاتِ الخطيرةِ مثلَ العملِ التجاريّ أو وقوعِ أضرارٍ كبيرةٍ ، قد تكونُ العقوبةُ أشد .

تهدفُ هذه القانونيَّةُ إلى حمايةِ سريَّةِ ونزاهةِ البياناتِ ومنعِ سوءِ استخدامِ التكنولوجيا المعلوماتيَّة ، و إنَّها تضمنُ أن يكونَ للأفرادِ والشركاتِ القدرةُ على حمايةِ بياناتِهم من الوصولِ والتجسّسِ غيرِ المصرَّح به وتضمنُ أن يكونَ هناكَ عواقبَ قانونيَّة مناسبة لأيّ خرقٍ للقانون .

و وفقاً للمادَّةِ /202 c/ من قانونِ العقوباتِ الألمانيّ(StGB) ، يُعاقَبُ على التحضيرِ لاستنساخِ واعتراضِ البياناتِ ، و تنطبق هذه الفقرةُ على مجالِ جرائمِ الحوسبةِ الإلكترونيَّةِ وانتهاكاتِ الخصوصيَّة .

تعني هذه المادَّةُ على وجهِ التحديدِ أنَّ تحضيرَ الأفعالِ الهادفةِ لاستنساخِ واعتراضِ البياناتِ هو جريمةٌ قابلةٌ للعقوبةِ ، حتَّى إنْ كان الاستنساخُ أو الاعتراضُ نفسه لم يحدث بعد ، و يهدفُ هذا القانونُ إلى منعِ هذه الأنشطةِ الجريمةَ في مراحلها الأولى وردعِ المتسبّبينَ المُحتَملين .

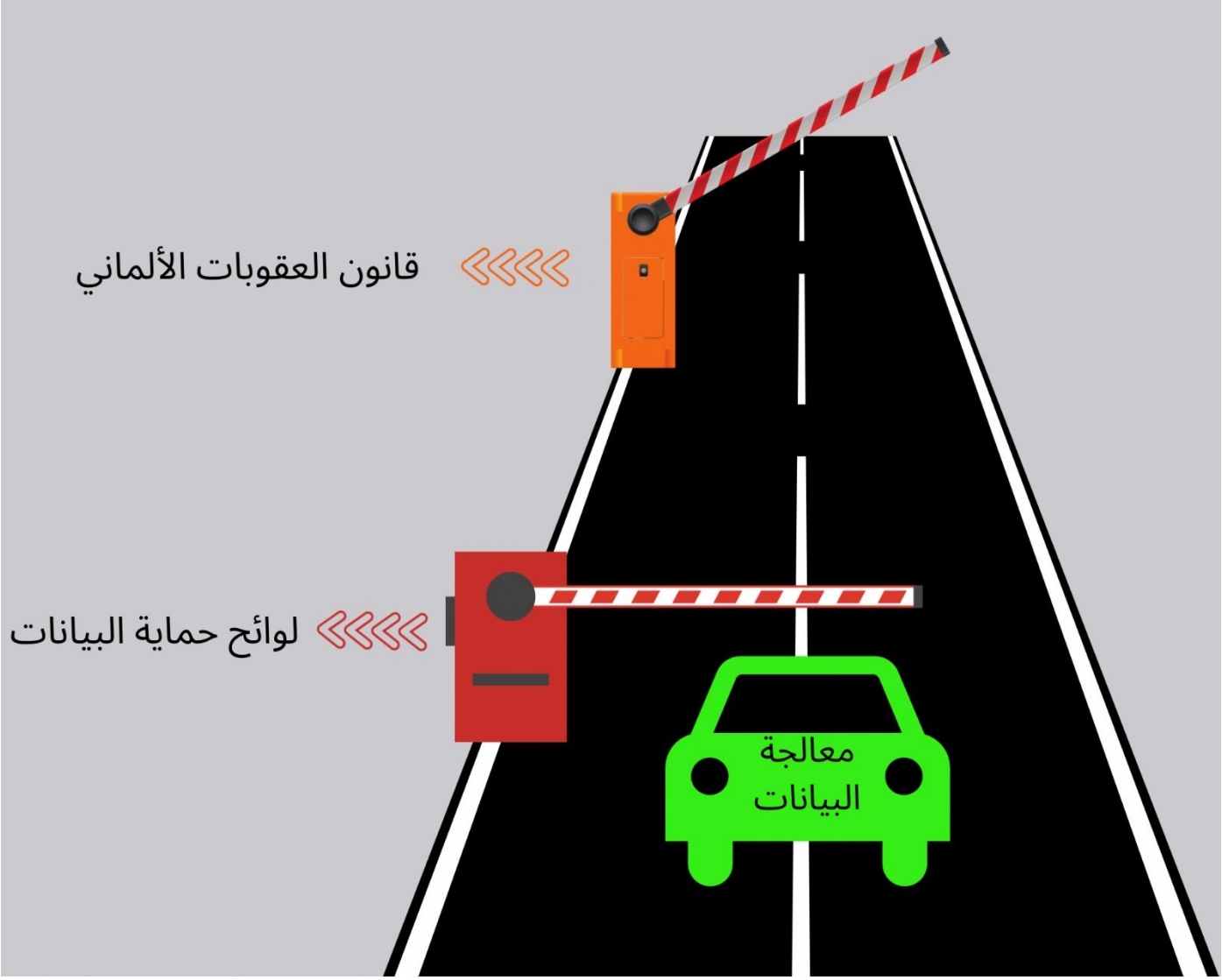
لشرحها بإيجازٍ فإنَّها معالجةُ البياناتِ قانونيَّاً اذا كان الحاجزانِ مفتوحانِ :

الحاجز الأول : هو لائحةُ حمايةِ البياناتِ أي أنْ تكونَ معالجةُ البياناتِ لها حجَّةٌ حسبَ واحدةٍ من المادتين السادسة أو التاسعة حسبَ اللوائحِ العامَّةِ لحمايةِ البيانات ، و في العادة يكونُ هذا الحاجزُ مغلقٌ لأنَّه لا يمكنُ معالجةُ البياناتِ بشكلٍ مشروعٍ إلَّا إذا كانَ المشرّعُ قد برَّرها مسبقاً و عندَ وجودِ المبرّرِ القانونيّ يكونُ هذا الحاجزُ مفتوحاً .

الحاجز الثاني : وهو قانونُ العقوباتِ أي أنْ تكونَ معالجةُ هذه البياناتِ قد ذكرَها المُشرّعُ بأنَّها عملٌ مخالفٌ للقانونِ وأخصُّ هنا المادة /203/ من قانونِ العقوباتِ ، و في العادة تكونُ هذه السكّةُ مفتوحةً بسببِ المادَّةِ الأولى من قانونِ العقوباتِ بأنَّه لا عقابَ من دونِ نصّ قانوني .

و تنصُّ المادَّةُ /1/ من قانونِ العقوباتِ على مبدأ قابليَّةِ المعاقبةِ ، وبموجبِ ذلك فإنَّ السلوكَ يُعدُّ جريمةً فقط إذا كانَ معاقباً صراحةً بموجبِ القانون ، وهذا يعني أنَّهُ يتطلَّبُ وجودَ أساسٍ قانوني لوجودِ جريمةٍ.

أي أنَّ السلوكَ يعدُّ معاقباً فقط إذا عرّفَ كجريمةٍ بموجبِ القانون ، و يُعرَّفُ هذا المبدأُ بمبدأ الشرعيَّةِ ، وهو أساسٌ مهمٌّ في القانونِ الجنائي ، و يضمنُ معاقبةَ شخصٍ فقط إذا مُنِعَ سلوكه صراحةً وبوضوحٍ قانوني .



الوحدةُ المعلوماتيَّة في سياقِ حمايةِ البياناتِ تشيرُ إلى مجموعةٍ مترابطةٍ من البياناتِ الشخصيَّةِ الَّتي تعملُ لتحقيقِ هدفٍ معيَّن أو وظيفةٍ محدَّدة ، إنَّها وحدةٌ منطقيَّةٌ أو تنظيميَّةٌ تجمعُ البياناتِ الشخصيَّةَ في ترتيبٍ معيَّن أو هيكلية .

تهدفُ الوحدةُ المعلوماتيَّة إلى ضمانِ حمايةِ البياناتِ وتمكينِ معالجةِ البياناتِ الشخصيَّةِ بطريقةٍ منظَّمةٍ وشفَّافة ، فهي تمكّنُ المسؤولينَ عن معالجةِ البياناتِ من جعلِ عمليَّةِ معالجةِ البياناتِ قابلةً للتتبع وتضمنُ حمايةَ الخصوصيَّةِ وحقوقَ الأفرادِ المعنيين .

إنَّ تعريفَ الوحدةِ المعلوماتيَّةِ وتنفيذّها يمكنُ أن يختلفَ بناءً على السياقِ والتشريعاتِ القانونيَّةِ المعمولِ بها ، وعادةً ما تشملُ الوحدةُ المعلوماتيَّةُ البياناتِ المرتبطةَ بفئةٍ معيَّنةٍ من الأفرادِ ، مثلَ العملاءِ أو الموظَّفينَ أو المرضى ، وتشملُ هذهِ البياناتُ أنواعاً مختلفةً من المعلوماتِ الشخصيَّةِ ، مثلَ الاسمِ، والعنوانِ ، وتاريخِ الميلادِ ، ومعلوماتِ الاتصالِ ، ومعلوماتِ الصّحةِ ، أو المعلوماتِ الماليَّة.

و منَ الضروريّ أنْ يكونَ لدى المسؤولينَ عن معالجةِ البياناتِ توجيهاتٌ وإجراءاتٌ واضحةٌ لتحديدِ وإدارةِ الوحداتِ المعلوماتيَّة ، ويتضمَّنُ ذلكَ تحديدَ الغرضِ والأساسَ القانونيَّ لمعالجةِ البياناتِ، وتحديدَ التدابيرِ الأمنيَّةِ المطلوبةِ ، وتحديدَ المسؤولياتِ وحقوقَ الوصولِ للأفرادِ المعنيّينَ ، وتحديدَ فتراتِ الاحتفاظِ وحذفِ البيانات.

تسهمُ الوحداتُ المعلوماتيَّةُ في تنفيذِ مبادئ حمايةِ البياناتِ مثل القيودِ المناسبةِ ، وتحديدَ الغرضِ، والشفافيَّةِ ، والمسائلةِ ، وتمكّنِ تنفيذِ فعَّالٍ لحقوقِ الأفرادِ المعنيّينَ فيما يتعلَّقُ بحمايةِ البياناتِ ، مثلَ حقّ الاطّلاعِ وتصحيحِ أو حذفِ البياناتِ الشخصيَّة.

و بشكلٍ عام ، فإنَّ تصوَّرَ الوحدةِ المعلوماتيَّةِ يسهمُ في حمايةِ الخصوصيَّةِ وتنفيذِ معالجةِ البياناتِ الشخصيَّةِ بطريقةٍ صحيحةٍ وفقاً للقوانينِ المعمولِ بها في حمايةِ البيانات.

يمكنُ وصفُ العيادةِ الفرديَّةِ في سياقِ حمايةِ البياناتِ كوحدةٍ معلوماتيَّةٍ ، إذ تشير العيادةُ الفرديَّةُ عادةً إلى عيادةٍ طبيَّةٍ أو عيادةٍ علاجيَّةٍ يتولَّاها فردٌ واحدٌ ، مثلَ الطبيبِ أو طبيبِ الأسنانِ أو المعالجِ النفسي.

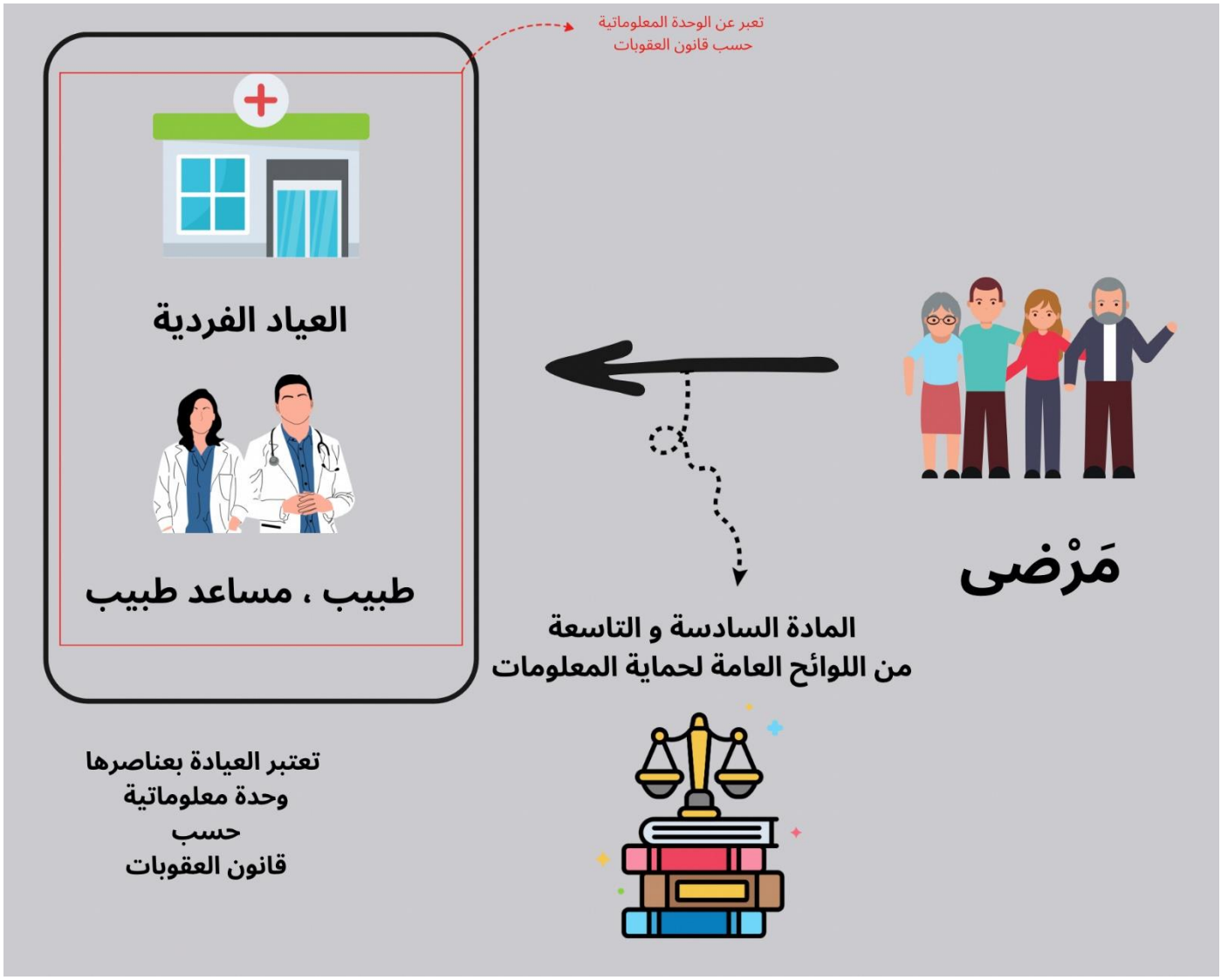
و كوحدةٍ معلوماتيَّة، تحتوي العيادةُ الفرديَّةُ على بياناتٍ ذاتِ صلةٍ بالأفرادِ ، تُجمَعُ و تُعالجُ وتخزَّنُ في إطارِ الرعايةِ الطبيَّةِ أو العلاجِ ، و يمكنُ أن تشملَ هذه المعلوماتُ مثلَ الأسماءِ ومعلوماتِ الاتّصالِ والتشخيصاتِ الطبيَّة وخططَ العلاجِ وسجلَّاتِ المرضى .

و يكونُ على العيادةِ الفرديَّةِ الامتثالُ لأحكامِ حمايةِ البياناتِ، خاصَّةً فيما يتعلَّقُ بسريَّةِ وسلامةِ وتوفّر البياناتِ الشخصيَّةِ و يشملُ ذلك اتّخاذَ تدابيرَ تقنيَّة وتنظيميَّة مناسبةٍ لحمايةِ البياناتِ من الوصولِ غيرِ المصرَّحِ به أو الفقدانِ أو الاستخدامِ غير المشروع.

بالإضافةِ إلى ذلك ، يجبُ اتّخاذُ الترتيباتِ المناسبةِ في العيادةِ الفرديَّةِ لضمانِ حقوقِ المرضى فيما يتعلَّقُ ببياناتِهم الشخصيَّةِ ، وتشملُ هذه الحقوقُ متطلَّباتِ المعلوماتِ حولَ معالجةِ البياناتِ، وحقَّ الوصولِ إلى البياناتِ، وتصحيحِها ، وحقّ الحذفِ أو تقييدها.

تتحمَّلُ العيادةُ الفرديَّةُ مسؤوليَّةَ استخدامِ بياناتِ المرضى فقط للأغراضِ الشرعيَّةِ وعدمَ نقلِها من دونِ موافقة ، ما لم يكن ذلك مطلوباً قانونيَّاً أو مبرَّراً بواسطةِ أساسٍ قانونيّ آخر.

و بشكلٍ عام ، تتحمَّلُ العيادةُ الفرديَّةُ كوحدةٍ معلوماتيَّةٍ مسؤوليَّةَ حمايةِ البياناتِ الشخصيَّةِ الَّتي تتعاملُ معها في إطارِ نشاطِها الطبيّ أو العلاجي.


تعبر عن الوحدة المعلوماتية
حسب قانون العقوبات
العياد الفردية
طبيب ، مساعد طبيب
مَرْضى
المادة السادسة و التاسعة
من اللوائح العامة لحماية المعلومات
تعتبر العيادة بعناصرها
وحدة معلوماتية
حسب
قانون العقوبات

يقومُ معالجونَ أو متخصّصونَ طبيّينَ آخرينَ بمشاركةِ عياداتهم سواءً من حيثُ الموقعِ أو التنظيمِ ، و يعدُّ هذا شكلاً من أشكالِ التعاونِ ، حيثُ يعملُ أعضاؤهُ بشكلٍ مستقل ، ولكنَّهم يشاركونَ في البنية التحتيَّةِ والموارد.

يمكنُ أن يتواجدَ في اتّحادِ الممارسةِ الطبيَّةِ تخصّصاتٌ طبيَّةٌ مختلفةٌ ، مما يوفّرُ للمرضى مجموعةً أوسعَ من الخدماتِ الطبيَّة ، و يحتفظُ كلُّ طبيبٍ أو معالجٍ بمسؤوليَّته المهنيَّةِ الخاصَّة واستقلاليته ، في حين يتعاونونَ في نفسِ الفضاءِ الطبيّ المشترك.

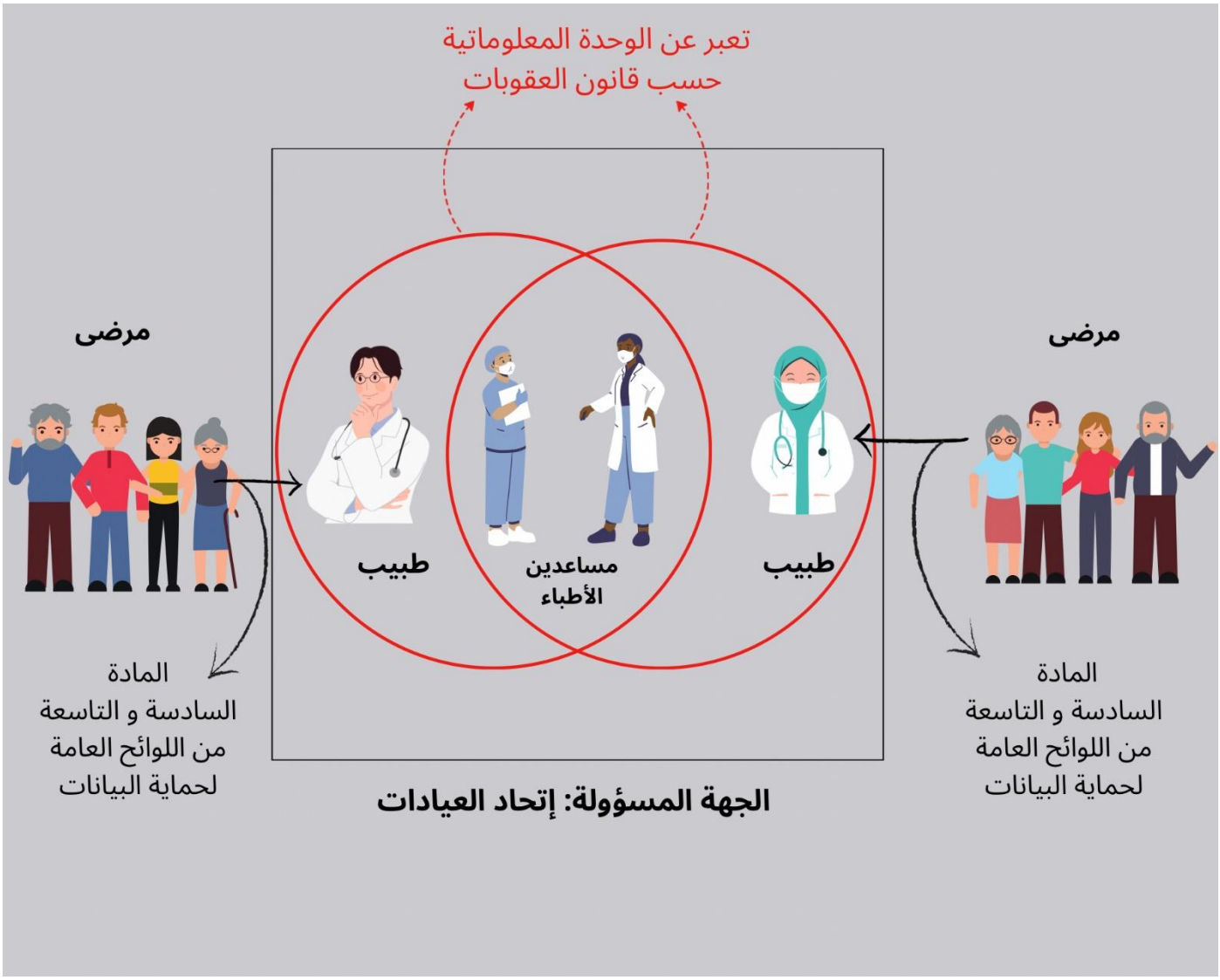
و يتيحُ اتّحادُ الممارسةِ الطبيَّةِ لأعضائِه مشاركةَ التكاليفِ والمواردِ مثلَ العنصرِ البشريّ والتجهيزاتِ التقنيَّة والمهامَ الإداريَّة.

أمَّا بالنسبةِ للمرضى ، فيوفّرُ اتّحادُ الممارسةِ الطبيَّةِ ميزة الوصولِ إلى مجموعةٍ أوسعَ من الخبراتِ الطبيَّة من دونِ الحاجةِ للذهابِ إلى أماكنَ مختلفة ، و يمكنُهم الاستفادةُ من الخبرةِ والمعرفةِ لأعضاءِ الاتّحاد المختلفين والحصول على رعايةٍ شاملةٍ في مكان واحد.

أمَّا من حيثُ حمايةِ البياناتِ ، فمن المهمّ أن تتَّخذَ التدابيرُ المناسبةُ في اتّحادِ الممارسةِ الطبيَّةِ لضمانش سريَّةِ وأمانِ البياناتِ الشخصيَّةِ للمرضى ، و يتضمَّنُ ذلك الامتثالَ للتشريعاتِ المتعلّقةِ بحمايةِ البيانات، وتنفيذَ إجراءاتِ الأمانِ لمنعِ الوصولِ غيرِ المصرَّحِ به، وتحديد المسؤولياتِ والاختصاصاتِ بوضوحٍ في التعاملِ مع البيانات .

باختصار، يعدُّ اتّحادُ الممارسةِ الطبيَّةِ شكلاً من أشكالِ التعاونِ والتنظيمِ في مجالِ الرعايةِ الصحيَّةِ ، حيثُ يشاركُ عدّة متخصّصين طبيّين مواردهم ويوفّرون رعايةً شاملةً للمرضى بشكلٍ مستقل عندَ كلّ طبيبٍ معالجٍ على حدى.

حيث يمثل كل طبيب معالج وحدة معلوماتية مستقلة.


تعبر عن الوحدة المعلوماتية
حسب قانون العقوبات
مرضى
مرضى
طبيب
مساعدين الأطباء
طبيب
المادة السادسة و التاسعة من اللوائح العامة لحماية البيانات
المادة السادسة و التاسعة من اللوائح العامة لحماية البيانات
الجهة المسؤولة: إتحاد العيادات

عيادةُ الممارسةِ المشتركةِ هي شكلٌ من أشكالِ التعاونِ في مجالِ الرعايةِ الصحيَّة ، حيثُ يعملُ عدَّةُ أطبَّاءٍ أو معالجون معاً في نفسِ الممارسةِ ، بدلاً من العملِ بشكلٍ فردي في ممارساتٍ منفصلةٍ ، يتعاونُ الأطبَّاءُ في ممارسةٍ مشتركةٍ ويشاركونَ الموارِدَ ، مثلَ المرافقِ والموظَّفينَ والتجهيزات الطبيَّة.

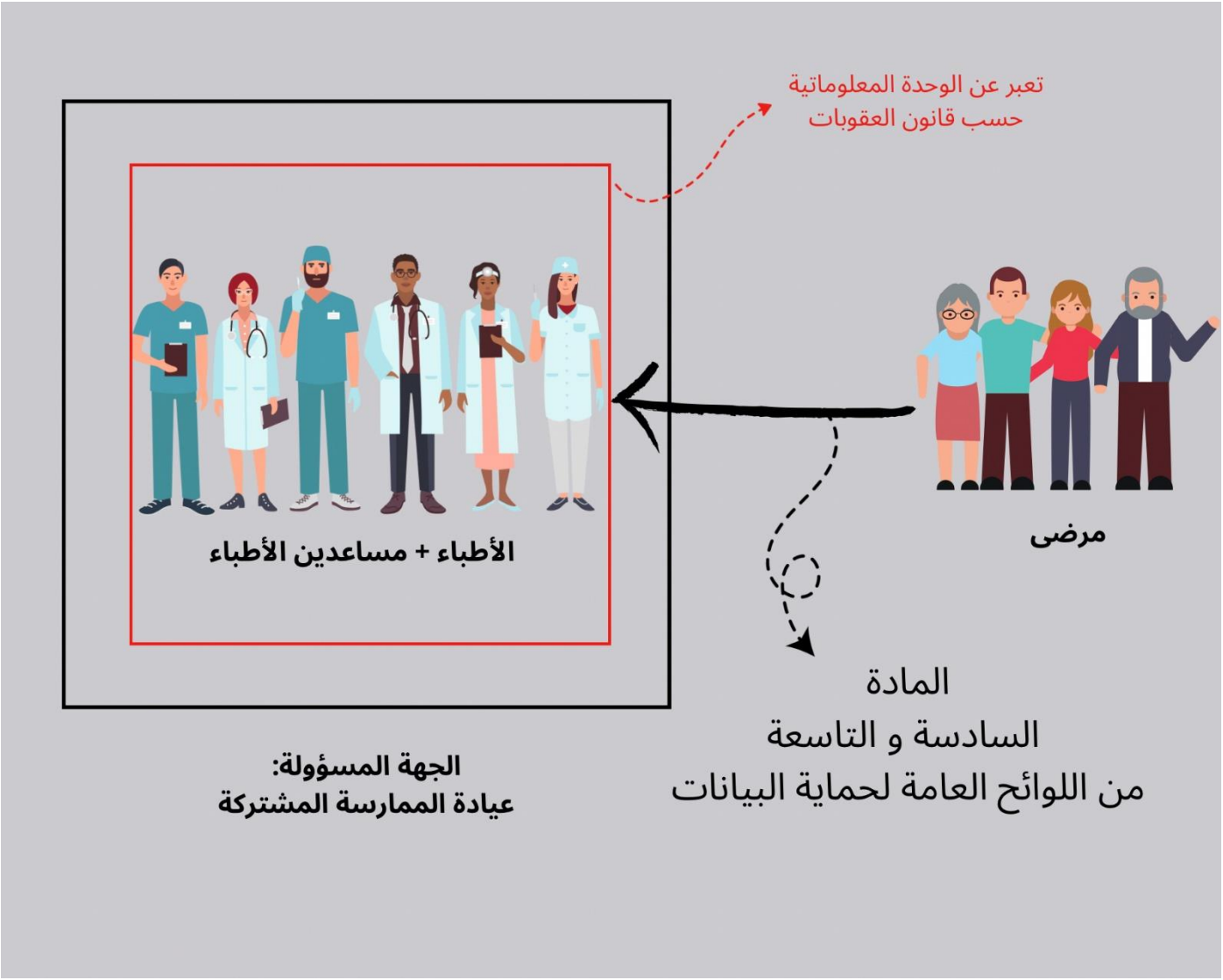
في ممارسةٍ مشتركةٍ ، يمكنُ أن تتواجدَ تخصّصاتٌ طبيَّةٌ مختلفةٌ ، ممَّا يوفّرُ للمرضى وصولاً إلى رعايةٍ صحيَّةٍ شاملةٍ ، و يحتفظُ كلُّ طبيبٍ بمسؤوليَّته المهنيَّةِ الخاصَّةِ وحريته ، في حين يتعاونونَ ويتشاركونَ الخبراتِ في نفسِ الممارسة.

تعتمدُ فوائدُ الممارسةِ المشتركةِ على إمكانيَّةِ تبادلِ المعرفةِ والخبرات بين الأطبَّاء وتقديمِ الدعم المتبادل ، و يمكنُ للأطبَّاءِ مشاركةُ المعلوماتِ والتجاربِ لتحسينِ رعايةِ المرضى ، بالإضافةِ إلى ذلك ، يمكن للممارسةِ المشتركةِ تحقيق كفاءة أعلى في إدارةِ الممارسةِ وتوفيرِ تكاليف.

فيما يتعلَّقُ بحمايةِ البيانات ، من المهم أن تتَّخذَ تدابير أمنيَّة مناسبة في الممارسة المشتركةِ لضمانِ سريَّةِ وأمانِ بياناتِ المرضى ، يشملُ ذلك التعاملَ الآمنَ مع المعلوماتِ الحساسة ، والامتثالِ للقوانين والتشريعاتِ المتعلّقةِ بحمايةِ البياناتِ ، وتنفيذِ إجراءات تقنيَّة وتنظيميَّة لحمايةِ البيانات.

و بشكلٍ عام ، تقدّمُ الممارسةُ المشتركةُ شكلاً من أشكالِ التعاونِ في مجالِ الرعايةِ الصحيَّةِ ، حيثُ يشتركُ الأطبَّاءُ في الموارِدِ لتوفيرِ رعايةٍ شاملةٍ للمرضى.

وهنا يشكّلُ جميعُ الأطبَّاءِ وحدةً معلوماتيَّة واحدة .


تعبر عن الوحدة المعلوماتية
حسب قانون العقوبات
مرضى
الأطباء + مساعدين الأطباء
المادة
السادسة و التاسعة
من اللوائح العامة لحماية البيانات
الجهة المسؤولة:
عيادة الممارسة المشتركة

المستشفى كوحدةٍ معلوماتيَّةٍ تعني تنظيمَ وإدارةَ بياناتِ المرضى داخلَ المستشفى ، و تتضمَّنُ هذه الوحدةُ جميعَ المعلوماتِ والبياناتِ ذاتِ الصلةِ الَّتي تُنتَجُ وتُجمَعُ وتُخزَّنُ وتُبَادّلُ في أثناءِ عمليَّةِ العلاج.

و كوحدةٍ معلوماتيَّةٍ ، يهتمُّ المستشفى بضمانِ سريَّةِ وأمانِ بياناتِ المرضى الشخصيَّةِ ، ويشملُ ذلك مثلاً التشخيصاتِ الطبيَّةَ وسيرَ العلاجِ والعلاجاتِ الدوائيَّة ونتائجَ التحاليلِ المخبريَّةِ وجميعَ البيانات الصحيَّةِ ذاتِ الصلة الأخرى.

يتحمَّلُ المستشفى مسؤوليَّةَ الامتثالِ للقوانينِ واللوائحِ المتعلّقةِ بحمايةِ البياناتِ وتنفيذِ التدابيرِ الأمنيَّةِ المناسبةِ لحمايةِ بياناتِ المرضى ، وتشملُ هذه الإجراءاتُ حمايةَ الوصولِ ، وتشفيرَ البياناتِ ، ونسخَ البياناتَ ، وتقييدَ الوصولِ للموظَّفينَ المخوّلينَ فقط ، وتدريبَ العاملين على قضايا حمايةِ البيانات.

بالإضافةِ إلى سريَّةِ وأمانِ بياناتِ المرضى ، تعدُّ إدارة وتنظيم هذه البيانات بشكلٍ فعَّال جانباً آخراً لوحدةِ المعلوماتِ في المستشفى ويشملُ ذلك التوثيقَ السليم ، وتبادلَ المعلوماتِ بأمانٍ بينَ الكوادرِ المعنيَّةِ ، وضمانَ توفّر البياناتِ لتوفيرِ الرعايةِ المستمرّةِ للمرضى.

و تعدُّ وحدةُ المعلوماتِ في المستشفى أمراً حاسماً لحمايةِ الخصوصيَّةِ وإدارةِ سلسةِ بيانات المرضى ، من خلالِ الامتثالِ للقوانينِ وتنفيذِ التدابيرِ الَّلازمةِ لحمايةِ البيانات ، و يضمنُ المستشفى سريَّةَ وسلامةَ وتوفُّرَ بياناتِ المرضى وبذلك تتعزَّزُ ثقةُ المرضى وتتحسَّن جودةُ الرعاية الطبيَّة.

المتعهّدونَ الخارجيُّونَ في قطَّاعِ الرعايةِ الصحيَّةِ هم الشركاتُ أو المؤسَّساتُ الَّتي تقدّمُ خدماتٍ ودعماً لمؤسَّساتِ الرعايةِ الصحيَّةِ ، ولكنَّها ليست جزءاً من التنظيمِ الداخليّ أو الهيكلِ الداخليّ لتلكَ المؤسَّسات. و عادةً ما يعملُ هؤلاءِ المتعهّدونَ بشكلٍ مستقلّ عن مؤسَّساتِ الرعايةِ الصحيَّةِ ويقدّمونَ خدماتٍ متخصّصةٍ في مجالاتٍ مختلفة.

وفيما يلي بعضُ أمثلةِ المتعهّدينَ الخارجيّينَ في قطَّاعِ الرعاية الصحيَّة:

١ .متعهّدو تكنولوجيا المعلومات : تقدّمُ هذه الشركاتُ البنيةَ التحتيَّةَ لتكنولوجيا المعلوماتِ والدعمَ الشبكيَّ وتطويرَ البرمجياتِ وغيرها من الخدماتِ المتعلّقةِ بتكنولوجيا المعلوماتِ للمستشفياتِ ، والعياداتِ ، والمنشآتِ الطبيَّةِ الأخرى.

٢ .المختبراتُ الطبيَّة : تقدّمُ المختبراتُ الخارجيَّةُ اختباراتٍ تشخيصيَّةً وفحوصاتٍ تستخدمُها المؤسَّساتُ الطبيَّةُ للحصولِ على تشخيصٍ دقيقٍ وتحسينِ رعايةِ المرضى.

٣ .خدماتُ التنظيفِ والصيانة : يتولَّى هؤلاءِ المتعهّدونَ مهامَ تنظيفِ وصيانةِ المستشفياتِ والعياداتِ والمنشآتِ الطبيَّةَ الأخرى لضمانِ بيئةٍ نظيفةٍ وآمنةٍ للمرضى والموظَّفينَ والزوَّار.

٤ .خدماتُ الرعاية الصحيَّة : مثلَ الخدماتِ المنزليَّةِ للرعايةِ الصحيَّةِ وعياداتِ العلاجِ الطبيعي أو الصيدليَّات الخارجيَّةِ الَّتي تقدّمُ رعايةً صحيَّةً خارجَ المستشفيات.

٥ .خدماتُ الأرشفةِ والوثائق : يهتمُّ هؤلاءُ المتعهّدونَ بتخزينِ وتصويرِ وإدارةِ السجلَّاتِ الطبيَّةِ وملفاتِ المرضى وغيرها من الوثائقِ في قطَّاعِ الرعاية الصحيَّة.

٦ .خدمات التدريب والتطوير : الشركاتُ الَّتي تقدّم التدريبَ والتطويرَ للموظَّفينَ الطبيّينَ لتوسيعِ معرفتِهم ومهاراتِهم وتعليمِ أفضلِ الممارساتِ الطبيَّةِ الحالية.

و تعاونُ المؤسَّساتِ الطبيَّةِ مع المتعهّدينَ الخارجيّينَ في قطَّاعِ الرعايةِ الصحيَّةِ يسمحُ لها بالاستفادةِ من الموارِدِ المتخصّصةِ والخبراتِ الَّتي قد لا تكونُ لديها داخليَّاً ، ومع ذلك فمنَ المهمّ التأكُّدُ من أنَّ هؤلاء المتعهّدينَ يلتزمونَ بأحكامِ حمايةِ البياناتِ والمتطلَّباتِ القانونيَّةِ الأخرى لضمانِ سريَّةِ وأمانِ بياناتِ المرضى.

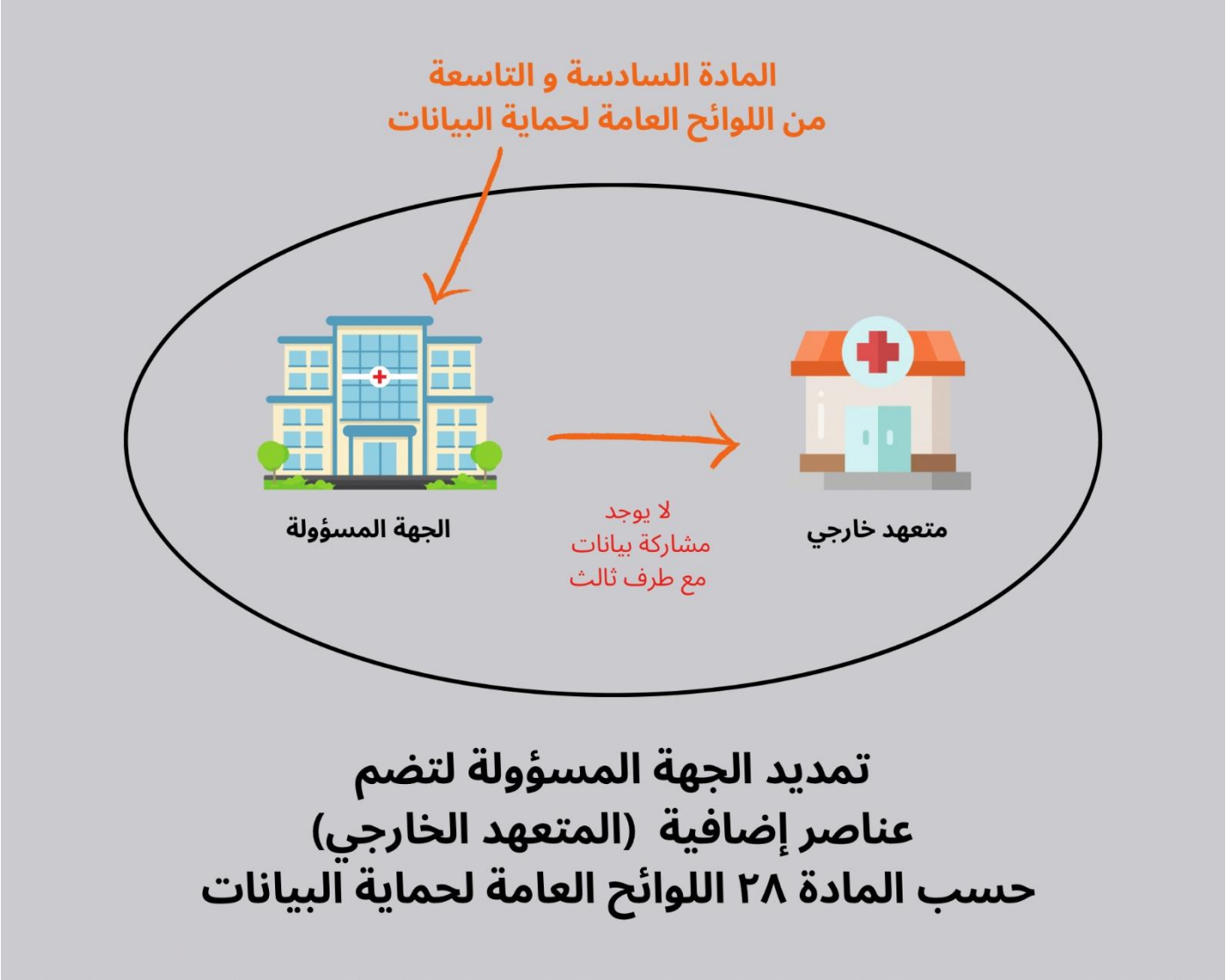
الحالة الأولى : المعالجةُ الَّتي تُبنَى على تعليماتٍ هي المعالجةُ الطلبيَّةُ الملزمَةُ بالتعليماتِ ، و تعدُّ مصطلحاً مهمَّاً في قانونِ حمايةِ البياناتِ ويشيرُ إلى معالجةِ البياناتِ الشخصيَّةِ بالنيابةِ عن شركةٍ أو منظَّمةٍ أخرى .

وفقًا للائحةِ العامَّةِ لحمايةِ البياناتِ في الاتّحادِ الأوروبي ، يُعدُّ وجودُ معالجةٍ طلبيَّةٍ ملزمَةٍ بالتعليماتِ عندما يُفوّض مُسؤولٌ معالجةَ البياناتِ الشخصيَّةِ إلى جهةٍ معالِجةٍ ، و تُعالجُ البياناتُ الشخصيَّةُ بناءً على التعليماتِ الصريحةِ من المسؤولِ فقط ولا يجوزُ لجهةِ المعالجةِ استخدامُ البياناتِ لأغراضِها الخاصَّة .
ويظلُّ المسؤولُ مسؤولاً عن معالجةِ البياناتِ ويجبُ عليه التأكُّدُ من أنَّ جهةَ المعالجةِ تتّخذُ التدابيرَ التقنيَّةَ والتنظيميَّةَ المناسبةَ لحمايةِ البيانات .

و لتنفيذِ المعالجةِ الطلبيَّةِ الملزمَة بالتعليماتِ بشكلٍ قانوني ، يجبُ على المسؤولِ وجهة المعالجةِ توقيعُ عقدٍ مكتوبٍ يلبّي متطلباتِ اللّوائحِ العامَّةِ لحمايةِ البياناتِ،و ينظّمُ هذا العقدُ المعالجةَ الطلبيَّةَ الملزمَة بالتعليماتِ بما في ذلكَ نوعُ وأغراضُ المعالجةِ ومدّةِ المعالجةِ وحقوقِ والتزاماتِ الطرفينِ بالإضافةِ إلى التدابيرِ المتعلّقةِ بحمايةِ البياناتِ وأمانِ البيانات.

يُعدُّ العملُ بالتعليماتِ ميزاناً هامَّاً يمكنُ من خلالِه للشركاتِ أنْ تُفوّضَ مهامَ معالجةِ البياناتِ الشخصيَّةِ إلى مقدّمي خدماتٍ خارجيّين متخصّصين ، مع ضمانِ التزامِ قواعدِ حمايةِ البياناتِ في الوقتِ نفسه .

باختصارٍ في هذه الحالةِ الجهةُ المسؤولةُ تتمدَّدُ لتضمَّ المتعهّدَ الخارجي فيصبحُ المتعّهدُ جزءً من هذه الجهة.



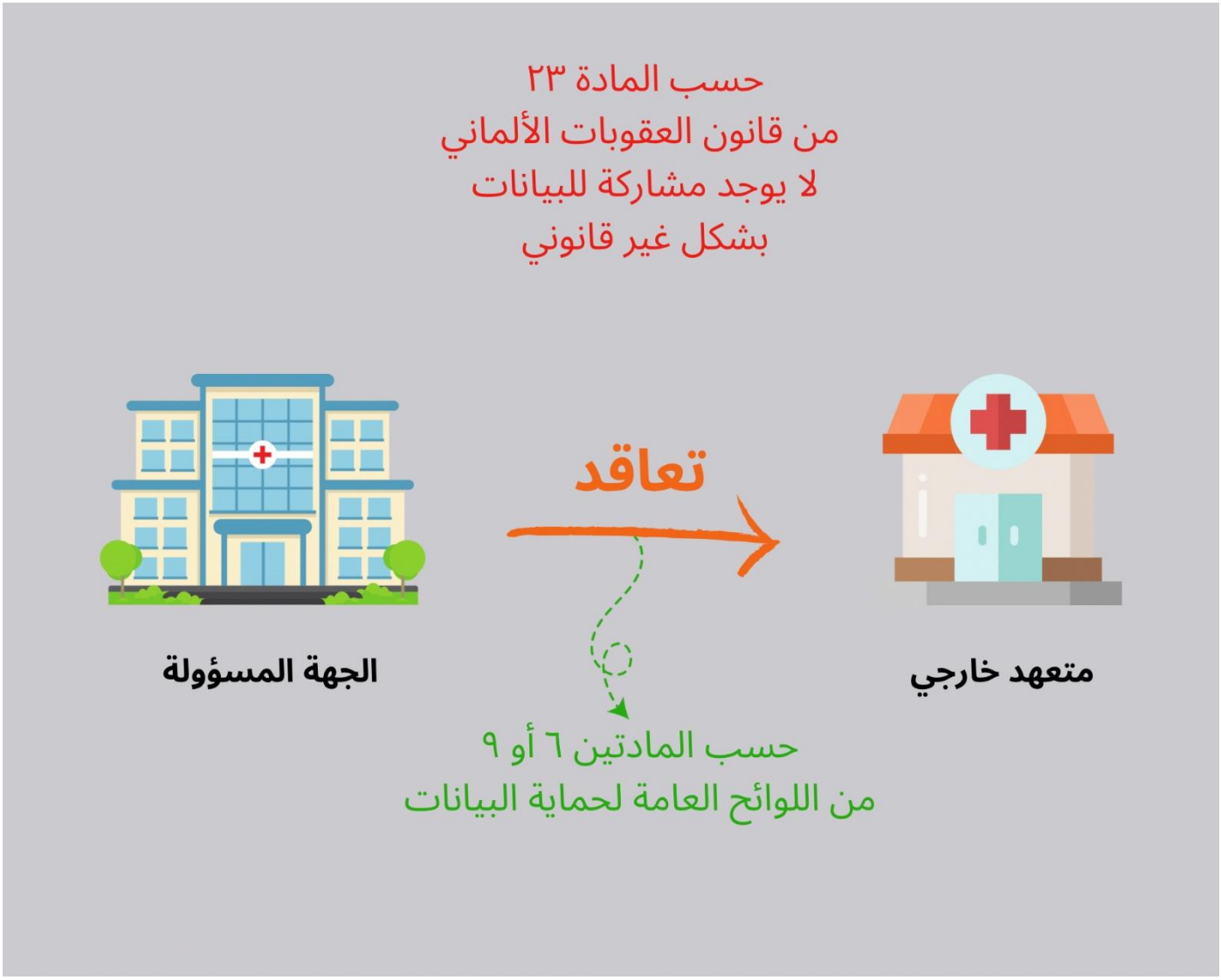
الحالة الثانية : المعالجةُ الطلبيَّةُ من دونِ توجيهٍ ، هي مصطلحٌ يشيرُ إلى الوضعِ الَّذي يكونُ فيه معالجُ البياناتِ بشكلٍ مستقلّ وغيرِ مرتبطٍ بتلقّي توجيهاتٍ من الجهةِ المسؤولةِ عن معالجةِ البياناتِ ، عندما تنفّذُ المعالجةُ الطلبيَّة ، يكونُ لدى معالجِ البياناتِ درجةً أكبر من الحريَّةِ في اتّخاذِ القراراتِ حولَ كيفيَّةِ معالجةِ البياناتِ الَّتي تحوَّلُ إليه ، و يعملُ المعالجُ بشكلٍ مستقلّ ويمكنُه الاستفادةُ من المعرفةِ الخاصَّةِ والخبرة المتخصّصة لتنفيذِ المهمة .

و من المهمّ أنْ نلاحظَ أنَّ المعالجةَ الطلبيَّةَ من دونِ توجيهٍ ليستْ ضروريَّةً دائماً ، و في بعضِ الحالات، قد يواصلُ الشخصُ المسؤولُ عن معالجةِ البياناتِ إصدارَ التوجيهاتِ أو الإرشاداتِ بشأنِ معالجةِ البياناتِ، حسبَ الاتّفاقاتِ المحدَّدةِ ومتطلَّباتِ قوانينِ حمايةِ البيانات .

و يمكنُ أن تحدثَ المعالجةُ الطلبيَّةُ من دونِ توجيه في سياقاتٍ مختلفة ، على سبيلِ المثال، وعندما تقومُ شركةٌ بتفويضِ مهامٍ معيَّنةٍ لمقدّم خدمةٍ خارجي يتمتَّعُ بالخبرةِ والكفاءةِ الَّلازمةِ لتنفيذِ هذه المهامِ من دونِ

تدخّلٍ مباشرٍ أو توجيهٍ من قبلِ الشركة ، ومع ذلك يجبُ الالتزامُ بالمتطلَّباتِ القانونيَّةِ وتحديداتِ حمايةِ البياناتِ لضمانِ أمانِ وحمايةِ البياناتِ الشخصيَّة.

و في هذه الحالة يتمُّ التعاقدُ بينَ الجهتين بحيثُ يبقى المتعهّدُ الخارجيُّ كجهةٍ منفصلةٍ تعالجُ البياناتُ بهدفِ إتمامِ هدفٍ مشروعٍ للجهةِ المسؤولة .



يمكنُ أنْ تشملَ مجموعةً متنوّعةً من المجالاتِ لضمانِ أمانِ وحمايةِ بياناتِ المرضى.

و إليكم بعضَ الأمثلة :

1ـ ضبطُ الوصول : وهو إنشاءُ آلياتٍ آمنةٍ لضبطِ الوصولِ مثلَ كلماتِ المرورِ ، والأرقامِ السريَّةِ ، أو البياناتِ الحيويَّةِ لتقييدِ وصولِ الأشخاصِ المخوّلينَ فقط إلى بياناتِ المرضى .

2ـ سياساتُ الخصوصيَّة : و هي وضعُ و تنفيذُ سياساتٍ وإجراءاتٍ واضحةٍ للخصوصيَّةِ تنظّمُ التعاملَ مع بياناتِ المرضى الحسَّاسةِ وتعزّزُ الوعيَ بقضايا حمايةِ البياناتِ بينَ الموظّفين .

3ـ التشفير : و هي تشفيرُ بياناتِ المرضى في أثناءِ التخزينِ ، والنقلِ ، والاتّصالِ لضمانِ حمايتِها من الوصولِ غيرِ المصرَّح به .

4ـ نسخ البيانات : وهو إجراءُ نسخٍ احتياطيّ لبياناتِ المرضى بشكلٍ منتظَمٍ لضمانِ استعادتِها في حالةِ فقدانِ البياناتِ أو تلفها .

5ـ الأمانُ الجسدي : و هو ضمانُ بيئةٍ آمنةٍ لتخزينِ بياناتِ المرضى مثل وصولِ الغرفِ الخاصَّةِ بالخوادمِ وتأمينِ الملفَّاتِ الورقيَّةِ ومنعِ وصولِ غيرِ المصرَّحِ به إلى الأجهزةِ الإلكترونيَّة .

6ـ التدريبُ والتوعيَّة : وهو تقديمُ تدريباتٍ للموظَّفينَ في العيادةِ لتوعيتِهم بأهميَّةِ حمايةِ البياناتِ وزيادةِ وعيِهم بالمخاطرِ المحتملّةِ وتدريبِهم على التعاملِ السليمِ مع بياناتِ المرضى .

7ـ ضابطُ حمايةِ البيانات : وهو تعيينُ ضابطِ حمايةِ البياناتِ المسؤولِ عن مراقبةِ وتنفيذِ إجراءاتِ حمايةِ البياناتِ في الوحدةِ المعلوماتيَّة .

8ـ تقليلُ البياناتِ: وهو ممارسةُ تقليل البيانات، إذ تُجمَعُ و تُخزَّنُ معلوماتٌ ضروريَّةٌ فقط للعلاجِ من أجل تقليلِ كميَّةِ البياناتِ المجمّعةِ ونطاقها .

9ـ اتفاقيَّاتُ معالجةِ البيانات : توقيعُ اتفاقيَّاتِ معالجةِ البياناتِ مع المزودين الخارجيين الَّذينَ يتمتّعونَ بحقّ الوصولِ إلى بياناتِ المرضى لضمانِ الامتثالِ لمعاييرِ حمايةِ البياناتِ المحدّدةِ اعتماداً على متطلَّباتِ وظروفِ الوحدةِ المعلوماتيَّة .

الدورةُ الحياتيَّة لبياناتِ المرضى

يُشيرُ مصطلحُ "الدورةِ الحياتيَّةِ لبياناتِ المرضى" إلى المراحلِ المختلفةِ الَّتي تمرُّ بها البياناتُ الشخصيَّةُ للمرضى في أثناءِ وجودها في سياقٍ طبّي أو صحي ، و تتضمَّنُ هذه الدورةُ الحياتيَّةِ عادةً المراحلَ الرئيسيَّةَ التالية :

1ـ جمعُ البيانات : في هذهِ المرحلةِ ، تُجمَعُ بياناتُ المرضى لأولّ مرَّة ، و يحدثُ ذلكَ عادةً عندما يلتحقُ المريضُ بمرفقٍ طبّي أو يطلبُ العلاجَ الطبيَ ، و خلالَ عمليَّةِ جمعِ البياناتِ ، تُجمعُ معلوماتٌ مختلفةٌ عن المريضِ ، مثل المعلوماتِ الشخصيَّةِ والتاريخِ الطبيَ والأعراضِ ونتائجِ التحاليل المخبريَّةِ وغيرها من البياناتِ الصحيَّة ذات الصلة .

2ـ معالجةُ وتخزينِ البياناتِ : بعدَ جمعِ البيانات ، تُعالَجُ في نظامِ معلوماتٍ طبيّ أو سجلّ طبيّ إلكتروني، و يتعيَّنُ في هذهِ المرحلةِ الالتزامُ بأحكامِ حمايةِ البياناتِ النافذةِ ، واتّخاذُ التدابيرِ الأمنيَّةِ اللَّازمةِ لضمانِ سريَّةِ وسلامةِ البيانات .

3ـ نقلُ البياناتِ وتبادلها : خلالَ دورةِ الحياةِ ، تُتبادَلُ بياناتُ المرضى بينَ مختلفِ المرافقِ الطبيَّةِ أو مقدّمي الخدماتِ الصحيَّة ، و يحدثُ ذلكَ غالباً عندما تتمُّ إحالةُ المريضِ من طبيبٍ إلى أخصائيّ آخر ، أو عندَ تبادلِ التقاريرِ الطبيَّةِ والتشخيصاتِ بينَ المستشفياتِ أو العيادات .

4ـ توافرُ البياناتِ والوصولُ إليها : طوالَ دورةِ الحياةِ ، يجبُ أن تكونَ بياناتُ المرضى متاحةً للمهنيّين الطبيّين المخوّلينَ لضمانِ تقديمِ الرعايةِ والعلاجِ المناسبين ، و في الوقتِ نفسه ، و من المهمّ تقييدُ الوصولِ إلى البياناتِ إلى أدنى حدّ ممكنٍ ، والتأكدُ من أنَّ الوصولَ إليها يتمُّ فقط بواسطةِ الأشخاصِ المخوّلين .

5ـ تحديثُ وحذفُ البيانات : يجبُ تحديثُ بياناتِ المرضى بانتظامٍ لضمانِ أنَّها حديثةٌ وصحيحةٌ ، و عندما لا تكونُ بعضُ البياناتِ ذاتِ الصلةِ بالمريضِ ضروريَّةً بعدَ الآن أو إذا طلبَ المريضُ ذلك ، يجبُ حذفُ البياناتِ وفقاً لأحكامِ حمايةِ البياناتِ النافذةِ أو جعلِها غيرِ قابلةٍ للتعقّب .

6ـ إتلافُ أو أرشفةُ البياناتِ : بعدَ انتهاءِ مدَّةِ الاحتفاظِ القانونيَّةِ أو عندما لم تعدْ البياناتُ مطلوبة ، يجبُ إتلافُ بياناتِ المرضى بطريقةٍ آمنةٍ ونهائيَّةٍ أو نقلِها إلى الأرشيفِ لضمانِ حمايةِ سريَّةِ وخصوصيَّةِ المرضى .

في مجالِ الرعايةِ الصحيَّةِ ، يمكنُ جمعُ ومعالجةُ مجموعةٍ من فئاتِ البياناتِ الشخصيَّةِ ، وتشملُ هذه الفئاتُ عادةً :

1- بياناتُ الصحة : تشملُ المعلوماتِ حولَ الحالةِ الصحيَّةِ الجسديَّةِ والعقليَّةِ للفرد ، مثلَ التشخيصات، و نتائجِ الفحوصاتِ الطبيَّة ، و خططِ العلاجِ ، و التقاريرِ الطبيَّة ، و وصفاتِ الأدوية .

2- بياناتِ التحقّقِ من الهويَّة : تشملُ المعلوماتُ الَّتي تستخدمُ لتحديدِ هويَّةِ الشخص ، مثلَ الاسم ، تاريخ الميلادِ ، و الجنس ، و رقم التأمينِ الاجتماعي ، و رقمِ الهويَّةِ الشخصيَّةِ والعنوان .

3- بياناتُ الاتّصال : تتضمَّنُ هذه البياناتُ المعلوماتِ المطلوبةَ للتواصلِ مع الفردِ ، مثلَ رقمِ الهاتفِ ، عنوانِ البريدِ الإلكترونيّ والعنوانِ البريدي .

4- البياناتُ الحسَّاسة : يمكنُ أن تشملَ البياناتُ الحسَّاسةُ معلوماتٍ تحتاجُ إلى حمايةٍ خاصَّة ، مثلَ معلوماتٍ عن الأصلِ العرقيّ ، والمعتقداتِ الدينيَّةِ أو العقائدِ الفلسفيَّة ، والبياناتِ الجينيَّةِ ، والبياناتِ البيومتريَّة (مثل بصماتِ الأصابع) ، وكذلكَ التوجّه الجنسي .

5- تاريخُ العلاجِ : تتضمَّنُ هذه الفئةُ معلوماتٍ عن العلاجاتِ الطبيَّة السابقة ، وفتراتِ الإقامةِ في المستشفى ، والعمليَّاتِ الجراحيَّةِ ، والأمراضَ السابقة.

6- بياناتُ التأمينِ والتسويَّة : تشملُ هذه الفئةُ المعلومات حولَ تأمينِ الشخصِ الصحي ، وبياناتِ التسويَّةِ الماليَّةِ للخدماتِ الطبية .

7- بياناتُ الطوارئ : في حالاتِ الطوارئ ، قد تكونُ المعلوماتُ الخاصَّةُ مثلَ الحساسيَّاتِ والأمراضِ السابقةِ والأدويةِ الحاليَّةِ ضروريَّةً لضمانِ توفيرِ الرعايةِ الطبيَّةِ السريعةِ والمناسبة .

و من الضروريّ أن يُتعّامَلَ مع هذه البياناتِ الشخصيَّةِ في مجالِ الرعايةِ الصحيَّةِ بمسؤوليَّةٍ واحترامٍ لتوجيهاتِ حمايةِ البياناتِ الساريةِ لضمانِ حمايةِ خصوصيَّةِ ومعلوماتِ المرضى الحسَّاسة .

عقدُ العلاج

يعَّرفُ عقدُ العلاجِ بأنَّهُ اتّفاقٌ قانونيٌّ بينَ المريضِ والطبيبِ ، أو أيّ ممارسٍ صحيّ آخر ، و يُحدَّدُ هذا العقدُ الشروطَ والحقوقَ المتعلّقةَ بالعلاجِ الطبيّ ويُحدّدُ المسؤولياتِ والواجباتِ للمريضِ والطبيبِ على حدّ سواء ، و يمكنُ أن يُوقَّعَ عقدُ العلاجِ شفهياً أو كتابيَّاً ، وعادةً ما يُنصَحُ بتوقيعِ عقدٍ كتابيّ لضمانِ الوضوحِ والقانونيَّة .

عقدُ العلاجِ النموذجيُّ يشملُ عادةً النقاطَ التالية :

1ـ نطاق الخدمة : يصفُ العقدُ نوعَ العلاجِ الطبيّ أو الخدمةَ الَّتي يقدّمُها الطبيبُ للمريضِ ، و قد يشملُ ذلكَ الرعايةَ العامَّة ، أو الفحصَ المحدَّدَ ، أو العمليَّةّ الجراحيَّة ، أو العلاجَ ، أو أيَّ إجراءٍ طبيّ آخر .

2ـ موافقةُ المريضِ : يعبّرُ المريضُ عن موافقتِه على العلاجِ ويوافقُ على الإجراءاتِ المُقترحةِ ، و يجبُ توفيرُ جميعِ المعلوماتِ الَّلازمةِ للمريضِ بشأنِ طبيعةِ العلاجِ ، والمخاطِرِ المحتملةِ ، والخياراتِ البديلة ، والنتائجَ المتوقَّعة .

3ـ السريَّة : يتضمَّنُ عقدُ العلاجِ عادةً أحكاماً بشأنِ سريَّةِ معلوماتِ المرضى ، و يلتزمُ الطبيبُ بالحفاظِ على خصوصيَّةِ وحمايةِ بياناتِ المرضى وفقاً للقوانينِ النافذةِ والمعاييرِ الأخلاقيَّةِ .

4ـ الأجرةُ وشروطُ الدفع : ينظّمُ العقدُ الاتّفاقاتِ الماليَّةَ بينَ المريضِ والطبيبِ ، بما في ذلكَ الأجرةَ المتّفقَ عليها للعلاجِ الطبيّ وشروطَ الدفع .

5ـ الحقوقُ والواجبات : لكلّ من المريضِ والطبيبِ حقوقٌ وواجباتٌ في إطارِ عقدِ العلاج ، و يحقُّ للمريضِ تلقّي رعايةٍ طبيَّةٍ مناسبةٍ ، وتوفيرَ معلوماتٍ حولَ حالتِه الصحيَّةِ وتلقّي العلاجِ بعنايةٍ ، و يتعيَّنُ على الطبيبِ تقديمُ أفضلِ رعايةٍ طبيَّةٍ ممكنةٍ ، وتوعيةَ المريضِ بشكلٍ مناسبٍ والالتزامَ بواجبِ الرعايةِ المطلوبة .

6ـ إنهاء العقد: يمكنُ إنهاءُ عقدِ العلاجِ في ظروفٍ معيَّنةٍ ، مثلَ الاتّفاقِ المُتبادلِ ، أو اكتمالِ العلاجِ ، أو تغييرِ الطبيبِ .

يُصنَّفُ هذا العقدُ حسبَ القانونِ المدنيّ الألماني أنَّه اتفاق خدمةٍ (عقد خدمي) ، وقد شرحَهُ المشرّعُ في المادةِ /611/.

في ألمانيا ، لا يوجدُ بشكلٍ عام إلزامٌ قانونيٌّ بتوقيعِ عقدِ العلاجِ كتابيَّاً للحصولِ على العلاجِ الطبيّ ، ومع ذلك فإنَّهُ من المعتادِ والمستحسنِ أنْ يتّفقَ الأطبَّاءُ والمرضى على عقدٍ شفهيّ أو كتابي لتحديدِ شروطِ وتوقّعاتِ العلاج .

و يهدفُ عقدُ العلاجِ إلى تنظيمِ حقوقِ وواجباتِ الطبيبِ والمريض وتوفيرِ أساسٍ واضحٍ للرعايةِ الطبيَّةِ، و من المهمّ أن يُبلَغَ الطبيبُ والمريضُ عن العلاجِ ، بما في ذلكَ نوعَ ومدى الإجراءاتِ المقرَّرةَ ، والمخاطرَ المحتملةَ والبدائلَ المُتاحة .

و قد يشملُ عقدُ العلاجِ أيضاً موافقةَ المريضِ على العلاجِ ومعالجةَ بياناتِهِ الشخصيَّةِ ، بالإضافةِ إلى ذلك قد يحتوي على أحكامٍ بشأنِ سريَّةِ المعلوماتِ الطبيَّةِ ، وطرائقِ الدفعِ ، وإنهاءِ العقد.

ومع ذلكَ فمنَ المهمّ أن نلاحظَ أنَّ بعضَ الخدماتِ الطبيَّةَ ، وخاصَّةً تلكَ الَّتي تنطوي على إجراءٍ جراحيّ أو حالةٍ خطرةٍ ، قد تتطلَّبُ موافقةً كتابيَّةً من المريضِ ، و في مثلِ هذه الحالاتِ، قد يكونُ من الضروريّ الحصولُ على عقدِ العلاجِ كتابيَّاً.

يُوصَى بأنْ تطلبَ من الطبيبِ عقدَ العلاجِ ، و توثيقَ جميعِ الشروطِ والاتّفاقاتِ بشكلٍ كتابيّ في حالةِ وجودِ عمليَّةٍ جراحيَّةٍ مخطَّطٍ لها أو علاج ، و ذلكَ يساعدُ على توفيرِ الوضوحِ والشفافيَّة .

تُنصُّ "المرجعيَّةُ النموذجيَّةُ لقوانينِ مزاولةِ مهنةِ الطبيبِ (MBO-Ä) "في ألمانيا على وجوبِ توثيقِ المعلوماتِ في العلاجِ الطبيّ ، وفقاً لل MBO-Ä، و يتوجَّبُ على الطبيبِ القيامُ بتوثيقٍ شاملٍ لضمانِ توفيرِ رعايةٍ طبيَّةٍ عاليةِ الجودةِ وضمانِ إمكانيَّةِ تتبّعِ الإجراءاتِ المُنفَّذةِ .

و تنصُّ ال MBO-Äعلى أنَّهُ يتعيَّنُ على الطبيبِ توثيقُ جميعِ بياناتِ العلاجِ الهامَّةِ ، بما في ذلكَ التشخيصاتِ ، والعلاجاتِ ، والأدويةَ ، ونتائجَ التحاليلِ ، ونتائج الفحوصاتِ ، ومعلوماتٍ أخرى ذاتِ صلة ، و يجبُ أن توثَّقَ في الوقتِ المناسبِ وبعنايةٍ وبشكلٍ يمكنُ تتبُّعه .

و تهدفُ واجباتُ التوثيقِ إلى الأغراضِ التالية :

1ـ استمراريَّةُ الرعاية : يتيحُ التوثيقُ الكاملُ والمفصَّلُ للأطبَّاءِ الآخرين متابعةَ علاجِ المريضِ والحصولَ على المعلوماتِ الهامَّةِ حولَ حالتِه الصحيَّةِ والإجراءاتِ المنفَّذة .

2ـ ضمانُ الجودة : يعملُ التوثيقُ على ضمانِ جودةِ الخدماتِ الطبيَّةِ المقدّمةِ والتحقّقَ منها ، و يسهمُ في تقييمِ وتحسينِ عمليَّاتِ العلاج .

3ـ الأمانُ القانونيُّ : يعدُّ التوثيقُ وثيقةً قانونيَّةً هامَّةً تُستخدَمُ كدليلٍ في حالةِ وجودِ نزاعاتٍ أو مسائلَ قانونيَّة ، و يمكنُ أن يساعدَ في إثباتِ مسؤوليَّةِ الطبيبِ والامتثالِ للمعاييرِ الطبيَّة .

4ـ حماية البيانات : عندَ التوثيقِ ، يتعيَّنُ على الطبيبِ الامتثالُ للقوانينِ الساريةِ لحمايةِ البياناتِ وضمانِ سريَّةِ بياناتِ المرضى .

و تختلفُ متطلَّباتُ التوثيقِ الدقيقةُ بناءً على الولايةِ وتخصّصِ الطبّ ، ولكنَّ المبادئَ العامَّةَ للتوثيقِ المنتبه والشاملِ والمفهومِ لا تزالُ قائمةَ لضمانِ توفيرِ رعايةٍ طبيَّةٍ عاليةِ الجودة .

و وفقاً **للمادةِ /630/ من القانونِ المدنيّ الألماني** ، فإنَّها تتعاملُ مع السجلّ الإلكترونيّ للمرضى ، تنصُّ هذه المادَّةُ على الحقوقِ والواجباتِ المتعلّقةِ بتوثيقِ المعلوماتِ الإلكترونيَّةِ لبياناتِ المرضى.

تشملُ المادَّةُ /630ف/ النقاطَ التالية :

1- إنشاءُ السجلّ الإلكترونيَ للمرضى : يُمكنُ من خلالِ هذه المادَّةِ إنشاءُ سجلّ إلكترونيّ للمرضى ، حيثُ تُخزَّنُ بياناتُ المرضى و تُدارُ إلكترونيَّاً ، و يهدفُ ذلكَ إلى تحسينِ توافرِ المعلوماتِ الطبيَّةِ وإمكانيَّةِ الوصولِ إليها للأطبَّاءِ والمعالجينَ ومقدّمي الخدماتِ الصحيَّةِ الأخرى ذاتِ الصلة .

2- حقوقُ المرضى : وفقاً للمادة /630ف/ من القانونِ المدني الألمانيّ ، فللمريضِ الحقُّ في معرفةِ نوعِ ومدى وغرضِ تخزينِ بياناتِه ، و يُمكنُ للمريضِ أن يوافقَ على تخزينِ واستخدامِ بياناتِه أو رفضها . بالإضافةِ إلى ذلك ، و للمريضِ الحقُّ في الاطّلاعِ على سجلّهِ الإلكترونيّ وطلبَ تصحيحِ أو حذفَ بياناتِ غيرَ صحيحةٍ أو غيرَ دقيقةٍ إن وجدت .

3- أمانُ البياناتِ وحمايةُ الخصوصيَّة : وفقاً للمادَّةِ /630ف/ من القانونِ المدنيّ الألمانيّ ، يجبُ على مقدّمي الخدماتِ الصحيَّةِ اتّخاذُ تدابيرَ تقنيَّةٍ وتنظيميَّةٍ ملائمةٍ لضمانِ أمانِ وسريَّةِ بياناتِ المرضى المخزّنَةِ إلكترونيَّاً ، و يجبُ حمايةُ بياناتِ المرضى من الوصولِ غيرِ المصرَّح به والفقدانِ أو الاستغلالِ غيرِ المشروعِ لها.

4- واجبُ التوثيق : يجبُ على مقدّمي الخدماتِ الصحيَّةِ توثيقُ بياناتِ المرضى إلكترونيَّاً .

و تعني **مسؤوليَّةُ الإثباتِ** على الأطبَّاءِ في حالاتِ النزاعاتِ القانونيَّةِ أنَّهُ في النزاعاتِ القانونيَّة ، يكونُ من مسؤوليَّةِ الطبيبِ إثباتُ أو دحضُ بعضِ الحقائقِ المحدّدة ، و يتحمَّلُ الطبيبُ مسؤوليَّةَ إثباتِ صحّةِ علاجهِ الطبيّ والامتثال لواجباتِه الطبيَّة .

و في النزاعاتِ القانونيَّةِ ذاتِ الصلةِ بالشؤونِ الطبيَّةِ ، يمكنُ أن تتعلَّقَ مسؤوليَّةُ الإثباتِ بجوانبَ مختلفة، مثل :

1- التشخيص : يجبُ على الطبيبِ أنْ يثبتَ صحّةَ تشخيصِهِ والتقديرَ الطبيّ المرتبطَ به ، إذ يجبُ عليه أنْ يقدّمَ أدّلةً على أنَّ التشخيصَ وضِعَ بناءً على معرفةٍ طبيَّةٍ متخصّصةٍ ونتائجِ فحوصاتٍ طبيَّةٍ مناسبة .

2- طرائق العلاج : عندما يتعلَّقُ الأمرُ باختيارِ وتطبيقِ طرائق العلاجِ المحدَّدةِ ، يكونُ على الطبيبِ مسؤوليَّةُ الإثباتِ ، إذ يجبُ عليهِ أنْ يوضّحَ أنَّهُ قامَ باتّباع معايير طبيَّةٍ ، و أنَّ الطرائقَ المُستخدمَةَ تتوافقُ مع المتطلّباتِ المهنيَّة .

3- الموافقةُ المطلعة : في حالةِ النزاعِ حولَ الموافقةِ المطلعةِ من قبلِ المريضِ على إجراءٍ طبيّ معيّن ، يكونُ على الطبيبِ مسؤوليَّةُ الإثباتِ ، و يجبُ عليه إثباتُ أنَّهُ أبلغَ المريضَ بشكلٍ مناسبٍ عن المخاطرِ والبدائلِ ، والنتائجِ المترتّبةِ على العلاجِ ، وأنَّهُ توجدُ موافقةٌ صحيحةٌ من المريضِ .

4- التوثيق : يعدُّ التوثيقُ الدقيقُ والشاملُ للإجراءاتِ الطبيَّةِ ، والتواصلُ مع المريضِ أمراً مهمَّاً ، و في حالةِ النزاع ، يكونُ من مسؤوليَّةِ الطبيبِ إثباتُ ما يتعلَّقُ بصحّةِ واكتمالِ المعلوماتِ الموثّقةِ .

و من المهمّ ملاحظةُ أنَّ توزيعَ المسؤوليَّةِ في حالاتِ الإثباتِ قد يختلفُ من حالةٍ لأخرى ويُعتمَدُ أيضاً على النظامِ القانونيّ المعمولِ به ، و في بعضِ الحالاتِ ، قد تُحوَّلُ المسؤوليَّةُ إلى المريضِ ، خاصَّةً عندما يتعلَّقُ الأمرُ بادّعاءاتِ الإهمالِ الجسيمِ أو أخطاءِ العلاج .

الحقوقُ والواجباتُ للتعاملِ مع بياناتِ المرضى

الاحتفاظُ بسجّلاتِ المرضى

تعني المادَّةُ /630ف / في القانونِ المدنيّ الألمانيّ أنَّ الطبيبَ المعالجَ ملزَمٌ بالاحتفاظِ بسجلِ المرضى لمدّةِ عشرِ سنواتٍ بعدَ انتهاءِ العلاجِ ، ما لم تنص القوانينُ الأخرى على وجوبِ الاحتفاظِ بها لفترةٍ أطول.

وفي هذا السياقِ ، فإنَّ "الملفَ الطبيَّ للمريضِ" هو مجموعةٌ من الوثائقِ والسجّلاتِ الَّتي تحتوي على معلوماتٍ طبيَّةٍ متعلّقةٍ بالمرضى ، مثلَ تاريخِ العلاجِ ، والتشخيصِ ، والتقاريرِ الطبيَّةِ و المعاملاتِ والوصفاتِ و أي سجلّاتٍ أخرى ذاتِ صلةٍ ، و يتضمَّنُ السجلُّ المتعلّقُ بالمرضى أيضاً الملاحظاتِ الشخصيَّةِ للطبيبِ ، والتفاصيل الأخرى المتعلّقةِ بالعلاج .

وهنا يجبُ توضيحُ بعضِ النقاطِ :

1ـ أنظمةُ المهنةِ الطبيَّةِ : تحدّدُ نقاباتُ الأطبَّاءِ المحلّيَّةُ في قوانينِها المهنيَّةِ عادةً فترةَ الاحتفاظِ بسجلَّاتِ الأطبَّاءِ ، و يمكنُ أنْ تختلفَ هذه القواعدُ حسبَ الولايةِ ، وتشملَ الوثائقَ الطبيَّة العامَّةَ والمجالاتِ الخاصَّة مثلَ الصورِ الشعاعيَّةِ أو تحاليلِ المختبرِ .. وفقاً للمادَّةِ 10 الفصل (3) من نموذجِ نظامِ المهنةِ الطبيَّةِ (MBO-Ä)، و يجبُ الاحتفاظُ بسجلَّاتِ الأطبَّاءِ لمدّةِ عشرِ سنواتٍ بعدَ انتهاءِ العلاجِ ، ما لم تنص القوانينُ القانونيَّةُ على وجوبِ الاحتفاظِ بها لفترةٍ أطول ، وهذه المدّةُ تنطبقُ على السجلَّاتِ الطبيَّةِ العامَّةِ، وقد تختلفُ قواعدُ الاحتفاظِ لبعضِ الوثائقِ الخاصَّةِ أو الحالاتِ الخاصَّة ، و ينصُّ هذا النصُّ على الفترةِ الدُنيا للاحتفاظِ بالسجلَّاتِ الطبيَّةِ ، ويمكنُ أن يكونَ هناكَ احتياجاتٌ قانونيَّةٌ خاصَّة تتطلَّبُ الاحتفاظَ بالسجلّاتِ لفترةٍ أطول .

2ـ فترةُ النقض : يعدُّ النقضُ عاملاً آخراً يؤثّرُ على فترةِ الاحتفاظِ بسجلّاتِ الأطبَّاءِ ، حيثُ تكونُ الفترةُ النصفيَّةُ لمطالباتِ التعويضِ العاديةِ عادةً ثلاثَ سنوات ، ولكنْ قد تكونُ أطولَ في حالاتٍ معيَّنةٍ ، و لذا يُنصحُ بالاحتفاظِ بالسجلّاتِ لفترةٍ مناسبةٍ لتغطيةِ أي مسائلَ قانونيَّةٍ محتملة .

3ـ سياساتُ المستشفى والعيادات : غالباً ما تحتوي المستشفياتُ والعياداتُ الطبيَّةُ على سياساتٍ داخليَّةٍ للاحتفاظِ بسجلّاتِ المرضى تتوافقُ مع المتطلَّباتُ القانونيَّةُ والمعاييرُ الطبيَّةُ ، و يمكنُ أن تحدّدَ هذه السياساتُ فتراتٍ محدَّدةً للاحتفاظِ بأنواعِ مختلفةٍ من الوثائقِ والسجلّات .

من الأهميَّةِ البالغةِ أنْ يُشَارَ إلى أنَّ مدّةَ الاحتفاظِ بسجلّاتِ الأطبَّاءِ تخدمُ في المقامِ الأوّل حمايةَ المرضى وتوفيرَ الرعايةِ المستمرة ، يجبُ حفظُ البياناتِ بشكلٍ آمنٍ وسري ، ويجبُ أن يكونَ التأكيدُ للوصولِ إليها مقصوراً على الأشخاص المصرَّحُ لهم فقط .

يَنصحُ الأطبَّاءُ والمنشآتُ الطبيَّةُ بالامتثالِ للقوانينِ القانونيَّةِ ذاتِ الصلة ، وقواعدِ المهنةِ والتوجيهاتِ ذاتِ الصلة ، من أجلِ ضمانِ أنَّ مدَّةَ الاحتفاظِ بسجلّاتِ الأطبَّاءِ تلبّي المتطلَّباتِ الساريةَ ، وتحقّقُ الحمايةُ الكافيةُ لخصوصيَّةِ المرضى واحتياجاتِ البيانات.

يعني تغييرُ بياناتِ المرضى في سياقِ حمايةِ البياناتِ الشخصيَّةِ أيَّ تعديلٍ ، أو تحديثٍ ، أو تعديلٍ للمعلوماتِ الشخصيَّةِ المتعلّقةِ بالمرضى ، و يمكنُ أن تشملَ هذه التغييراتُ كلَّ السجلَّاتِ الرقميَّةِ، والسجلّاتِ الورقيَّة .

في سياقِ حمايةِ البياناتِ ، من المهمّ أن تُغيَّرَ بياناتُ المرضى وفقاً للقوانينِ ، واللوائحِ النافذةِ في مجالِ حمايةِ البياناتِ ، ويشملُ ذلك على وجهِ الخصوصِ اللائحةَ العامَّةَ لحمايةِ البياناتِ في الاتّحادِ الأوروبيّ وقانونَ حمايةِ البياناتِ الاتّحادي في ألمانيا .

يجبُ أنْ تُغيَّر بياناتُ المرضى فقط في الحالاتِ المسموحِ بها قانونيَّاً، مثلَ :

1ـ موافقةُ المريضِ : إذا قدَّمَ المريضُ موافقتَه الصريحةَ على تغييرِ بياناتِه، يمكنُ تنفيذُ ذلكَ وفقاً للوائحِ حمايةِ البياناتِ النافذةِ .

2ـ الامتثالُ للالتزاماتِ القانونيَّةِ : في بعضِ الحالاتِ ، قد يكونُ من الضروريّ تغييرُ بياناتِ المرضى للامتثالِ لمتطلَّباتِ قانونيَّةٍ ، مثلَ التقاريرِ والتوثيقاتُ اللَّازمةِ في قطَّاعِ الرعايةِ الصحيَّة .

3ـ تصحيحُ المعلوماتِ الخاطئةِ : إذا كانَتْ هناكَ أخطاءٌ أو تناقضاتٌ في بياناتِ المرضى ، فيمكنُ تصحيحُها لضمانِ دقّةِ واكتمالِ المعلومات .

مع ذلكَ ، فمنَ المهمّ ملاحظةُ أنَّ تغييرَ بياناتِ المرضى غيرِ المصرَّحِ به ، مثلَ الحذفِ غيرِ المصرَّحِ به أو التلاعبِ أو التزويرِ ، يعدُّ انتهاكاً لحمايةِ البياناتِ وقد يكونُ له عواقبُ قانونيَّة .

و تعدُّ حمايةُ بياناتِ المرضى والحفاظُ على الخصوصيَّةِ هما الهدفان الرئيسيانِ لحمايةِ البيانات الشخصيَّةِ في قطَّاعِ الرعايةِ الصحيَّةِ ، لذا ينبغي أنْ تُغيَّرَ بياناتُ المرضى فقط من قِبلِ الأشخاصِ المخوّلُ لهُم بذلك وفقاً للوائحِ حمايةِ البياناتِ النافذةِ ، وبمراعاةِ حقوقِ ومصالحِ المرضى.

يعني الإفصاحُ الداخليُّ لبياناتِ المرضى نقلَ المعلوماتِ والبياناتِ المتعلّقةِ بالمرضى داخلَ نفسِ المنظَّمةِ أو المؤسَّسةِ في قطَّاعِ الرعايةِ الصحيَّةِ ، و يمكنُ أنْ يحدثَ ذلكَ داخلَ مستشفى أو عيادةٍ طبيَّةٍ أو مركزٍ طبيّ آخر .

الإفصاحُ الداخليُّ لبياناتِ المرضى هو جزءٌ هامٌّ من الرعايةِ الصحيَّةِ وتنسيقِ العلاجِ ، و يُسمَحُ بتوفيرِ المعلوماتِ اللَّازمةِ للمتخصّصينَ والموظَّفينَ المعنيّينَ لضمانِ تقديمِ رعايةٍ مناسبةٍ ومنسَّقةٍ.

و عندَ القيامِ بالإفصاحِ الداخليّ لبياناتِ المرضى ، من المهمّ أنْ يُحَافَظَ على سريَّةِ المعلوماتِ والحمايةِ اللَّازمةِ للخصوصيَّةِ ، و يعني ذلكَ أنَّ الوصولَ إلى بياناتِ المرضى يجبُ أن يكونَ مقصوراً على الأشخاصِ المخوّلِ لهم فقط ، والمشاركينَ في العلاجِ المباشرِ أو الرعايةِ للمريضِ ، ويهدفُ ذلك إلى ضمانِ حمايةِ خصوصيَّةِ المرضى ومنعِ الوصولِ غيرِ المصرَّحِ به أو الكشفِ عن المعلوماتِ الحسَّاسة.

يجبُ أن تتَّخذَ المنظَّماتُ في قطَّاعِ الرعايةِ الصحيَّةِ التدابيرَ الأمنيَّةَ اللَّازمةَ لضمانِ أنَّ الإفصاحَ الداخليَّ لبياناتِ المرضى يحدثُ في بيئةٍ آمنةٍ ، وتشملُ هذه التدابيرُ تنفيذَ آلياتِ التحكّمِ في الوصولِ وتقنيَّاتِ التشفيرِ وتدريبِ الموظَّفينَ لزيادةِ الوعي بحمايةِ البياناتِ .

علاوةً على ذلك ، يجبُ إبلاغُ المرضى بالإفصاحِ الداخليّ لبياناتِهم ، ويجبُ أن يكونَ لهم الحقُّ في إبداءِ موافقتِهم أو رفضِهم ، و يمكنُ تحقيقُ ذلكَ من خلالِ التوعيةِ بممارساتِ حمايةِ البياناتِ وتوفيرِ نماذجِ الموافقةِ ، و تنبعُ الإجراءاتُ الداخليَّةُ للكشفِ عن بياناتِ المرضى من الحاجةِ إلى تنظيمِ وتسهيلِ تدفّقِ المعلوماتِ في إطارِ الرعايةِ الصحيَّةِ الداخليَّةِ ، و يتضمَّنُ ذلكَ تبادلَ المعلوماتِ بينَ الأطبَّاءِ والممرّضينَ والموظَّفينَ الصحيّينَ الآخرينَ داخلَ نفسِ المؤسَّسةِ الطبيَّةِ.

وتكونُ هذه الإجراءاتُ ضروريَّةً لتوفيرِ الرعايةِ المتكاملةِ وتحسينِ التنسيقِ بينَ أعضاءِ الفريقِ الطبي.

و تتطلَّبُ الكشوفاتُ الداخليَّةُ للمرضى الحفاظَ على خصوصيَّةِ وسريَّةِ المعلوماتِ الطبيَّةِ ، ويجب أن تُنَفَّذَ هذه الكشوفاتُ بموجبِ قوانينِ حمايةِ البياناتِ النَّافذةِ وتوجيهاتِ الخصوصيَّةِ الصحيَّةِ ، و يتعيَّنُ على جميعِ

الأشخاصِ الَّذينَ يشاركون َفي هذه الكشوفاتِ أن يكونوا **ملتزمينَ بالسريَّةِ** وأنْ يتّبعوا سياساتِ وإجراءاتِ الخصوصيَّةِ المعمولِ بها .

ومن أمثلةِ الكشوفاتِ الداخليَّةِ للمرضى تبادلُ المعلوماتِ بينَ الأطبَّاءِ المعالجينَ والأخصَّائيّينَ الآخرينَ الَّذينَ يشاركونَ في الرعايةِ الصحيَّةِ للمريضِ ، و يشملُ ذلكَ تبادلَ التشخيصاتِ ، والتحاليلَ والأدويةَ ، وتقاريرَ العمليَّاتِ والإجراءاتِ الطبيَّةَ الأخرى ، و يساعدُ هذا النوعُ من الكشوفاتِ الداخليَّةِ في تحسينِ تنسيقِ العنايةِ الصحيَّةِ وتوفيرِ الرعايةِ الملائمةِ للمرضى .

وفي سياقِ حمايةِ البياناتِ ، تُطبَّقُ الإجراءاتُ التقنيَّةُ والتنظيميَّةُ لحمايةِ البياناتِ الطبيَّةِ في أثناءِ الكشوفاتِ الداخليَّةِ ، و يتضمَّنُ ذلكَ تنفيذَ الإجراءاتِ الأمنيَّةِ وضمانَ تقييدِ الوصولِ إلى المعلوماتِ الحسَّاسةِ .

تتمتَّعُ مشاركةُ معلوماتِ المرضى مع الأقاربِ في ألمانيا بحمايةٍ قانونيَّةٍ وتنظم وفقاً لقانونِ حمايةِ البياناتِ الاتحاديّ (BDSG) ، وقانونِ الضمانِ الاجتماعيّ (SGB) ، ووفقاً لهذهِ الأنظمةِ القانونيَّةِ ، تنطبقُ المبادئ التاليةُ على مشاركةِ معلوماتِ المرضى مع الأقارب :

1ـ موافقةُ المريضِ : في المبدأ ، تتطلَّبُ مشاركةُ معلوماتِ المرضى مع الأقاربِ موافقةً صريحةً من المريضِ ، و يحقُّ للمريضِ أنْ يقرّرَ أنَّ المعلوماتِ الطبيَّةِ يمكنُ مشاركتُها مع الأقاربِ ، ولمن يمكنُ أنْ يوافقَ كتابيَّاً أو شفهيَّاً .

2ـ حالاتُ الطوارئ : في حالاتِ الطوارئ الحياتيَّةِ الَّتي لا يكونُ فيها المريضُ قادراً على إعطاءِ موافقتِه، يمكنُ مشاركةُ معلوماتِ المرضى مع الأقاربِ إذا كانَ ذلكَ ضروريَّاً لتأمينِ الرعايةِ الطبيَّةِ المناسبةِ ، و ينطبقُ هذا بشكلٍ خاصّ عندما يكونُ من الضروريّ مشاركةُ المعلوماتِ لإنقاذِ الحياةِ أو منعِ حدوثِ أضرارٍ صحيَّةٍ خطيرةٍ .

3ـ توكيلُ الرعايةِ وتصريحُ المريضِ : إذا وكّلَ المريض شخصاً آخراً بتمثيلِه في حالةِ عدمِ قدرتِه على اتّخاذِ قراراتٍ ، أو إذا أصدرَ تصريحاً صحيَّاً ، فيمكنُ تحديدُ من يحقُّ له الوصولُ إلى معلوماتِه الطبيَّةِ من خلالِ هذه الوثائقِ ، و في هذه الحالةِ ، يجبُ على الأطبَّاءِ المعالجينَ الالتزامُ بتوجيهاتِ هذهِ الوثائقِ.

4ـ استثناءاتٌ قانونيَّة : هناكَ بعضُ الاستثناءاتِ القانونيَّةِ الَّتي تسمحُ بمشاركةِ معلوماتِ المرضى مع الأقاربِ من دونِ موافقةٍ صريحةٍ من المريضِ .

والمثالُ على ذلكَ هو التزامٌ قانونيٌّ بالإبلاغِ عن بعضِ الأمراضِ المعديةِ ، حيثُ يكونُ من الضروريّ مشاركةُ البياناتِ مع الجهاتِ الصحيَّةِ أو الجهاتِ الحكوميَّةِ الأخرى.

ومع ذلك ، منَ المهمّ أن نلاحظَ أنَّ مشاركةَ معلوماتِ المرضى مع الأقاربِ يجبُ أنْ تتوافقَ مع مبادئِ حمايةِ البياناتِ وسريَّةِ الطبيبِ ، و يجبُ أن تُشَارَكَ فقط بالحدّ الَّذي يكونُ ضروريَّاً لتقديمِ الرعايةِ الطبيَّةِ والدعم المناسب للمريض .

يُوصَى بأنْ يلتزمَ الأطبَّاءُ والفريقُ الطبيُّ بالقوانينِ والتنظيماتِ المعمولِ بها فيما يتعلّقُ بمشاركةِ معلوماتِ المرضى مع الأقاربِ ، وأنْ يتواصلوا مع المسؤولينَ القانونيّينَ أو استشاريّين قانونيّينَ للحصولِ على التوجيهاتِ الَّلازمةَ في حالةِ وجودِ أيّ استفساراتٍ أو قضايا قانونيَّةٍ محدَّدة .

تتمُّ عمليَّةُ تبادلِ بياناتِ المرضى بينَ طبيبِ العائلةِ والمستشفى في ألمانيا وفقاً لأحكامِ قانونِ حمايةِ البياناتِ الاتحاديّ (BDSG) قانونُ الضمانِ الاجتماعي .(SGB) فيما يلي بعضُ النقاطِ الهامَّةِ للاعتبار :

1ـ موافقةُ المريض : يتطلَّبُ تبادلُ بياناتِ المرضى بين طبيبِ العائلةِ والمستشفى عادةً موافقةً صريحةً من المريضِ ، و يجبُ أن يكونَ المريضُ مطّلعاً وموافقاً على أنَّ معلوماتِه الطبيَّةَ يمكنُ تبادلُها بينَ المؤسّساتِ الطبيَّةِ المعنية .

2ـ تحديدُ الغرض : يجبُ أنْ تُتَبَادلَ البياناتُ فقط لأغراضِ الرعايةِ الصحيَّةِ والعلاجِ المناسبِ للمريضِ ، و لا يجوزُ استخدامُ البياناتِ المرسلةِ لأغراضٍ أخرى من دونِ الحصولِ على موافقةِ المريض .

3ـ أمانُ البيانات : يجبُ اتّخاذُ التدابيرِ المناسبةِ لضمانِ أمانِ وسريَّةِ بياناتِ المرضى في أثناءِ عمليَّةِ التبادلِ ، و يمكنُ أنْ تشملَ هذه التدابيرُ استخدامَ قنواتِ اتّصالٍ آمنةٍ أو تطبيقَ تقنيَّاتِ التشفير.

4ـ واجبُ السريَّةِ للطبيبِ : يخضعُ الأطبَّاءُ والموظَّفونَ الطبيّونَ لواجبِ السريَّةِ الطبيَّةِ ولا يجوزُ لهم إفشاءُ بياناتِ المرضى إلَّا وفقاً للقوانينِ ، و ينطبقُ هذا الالتزامُ بالسريَّةِ أيضاً على عمليَّةِ تبادلِ البياناتِ بينَ طبيبِ العائلةِ والمستشفى .

5ـ التوثيق : يجبُ توثيقُ عمليَّةِ التبادلِ بشكلٍ سليمٍ لتكونَ مسجّلةً وقابلةً للتتبع ، و يشملُ ذلك تسجيلَ عملياتِ نقلِ البياناتِ وموافقةَ المريضِ وأي معلوماتٍ أخرى ذاتِ صلة .

تنصُّ المادَّةُ /73/ الفقرةُ /1/ البند /ب/ من قانونِ الضمانِ الاجتماعيّ الخامسِ على أنَّه

يتعيَّنُ على مقدّمي الخدماتِ الطبيَّةِ الَّذينَ يعالجونَ المؤمَّنَ عليهِم أن يسألوا المؤمَّنَ عليه

عن طبيبِ العائلةِ الَّذي اختارهُ ، و إنَّهُم ملزَمُونَ بنقلِ بياناتِ ونتائجِ الفحوصِ الطبيَّةِ والمعلوماتِ الخاصَّةِ بالمؤمَّنِ عليهِ بموافقتِه لأغراضِ التوثيقِ والعلاجِ المستقبليّ الَّذي سيتمُّ تقديمُه لدى طبيبِ العائلةِ ، و يجبُ على طبيبِ العائلةِ بموافقةِ المؤمَّنِ عليهِ ، نقلُ البياناتِ و النتائجِ الَّلازمةِ للعلاجِ إلى مقدّمي الخدماتِ الطبيَّةِ الَّذينَ يعالجونَ المؤمَّنَ عليه عندَ تغييرِ طبيبِ العائلةِ ، و يتعيَّنُ على الطبيبِ السابقِ ، بموافقةِ المؤمَّنِ عليه ، أنْ ينقلَ الملفّاتِ المخزَّنةَ لديه بشأنِ المؤمَّنِ عليه بالكامل إلى الطبيبِ الجديد .

تتطلَّبُ هذه المادَّةُ من مقدّمي الخدماتِ الصحيَّةِ الالتزامَ بتبادلِ المعلوماتِ بموافقةِ المؤمَّنِ عليهِ وفقاً للحفاظِ على استمراريَّةِ الرعايةِ الصحيَّةِ ، وتنسيقُها بينَ مختلفِ المقدّمين ، و الهدفُ من هذهِ المتطلَّباتِ إلى ضمانِ تدفّقِ المعلوماتِ الطبيَّةِ الَّلازمةِ بينَ الفريقِ الطبيّ وتوفير الرعايةِ الصحيَّةِ الشاملةِ والمتكاملةِ للمؤمَّنِ عليه ، و يُعَدُّ الحفاظُ على خصوصيَّةِ وسريَّةِ بياناتِ المرضى والالتزامُ بتوجيهاتِ حمايةِ البياناتِ جزءاً أساسيَّاً من تنفيذِ هذهِ المادَّة .

تتعلَّقُ عمليَّةُ تبادلِ البياناتِ بينَ شركاتِ التأمينِ الصحيّ والمؤسَّساتِ الطبيَّةِ بتبادلِ المعلوماتِ الطبيَّةِ ذاتِ الصلةِ ، و بياناتِ التسويةِ الماليَّةِ بينَ الجانبينِ ، و يعدُّ هذا التبادلُ أمراً هامَّاً لضمانِ تسويةِ التكاليفِ الطبيَّة واستردادِها بطريقةٍ مناسبةٍ ، وفيما يلي بعضُ الجوانبِ الهامَّةِ لعمليَّةِ تبادلِ البيانات :

1ـ المعلوماتُ الطبيَّةُ : تقومُ المؤسَّسةُ الطبيَّةُ بإرسالِ المعلوماتِ الطبيَّةِ المتعلّقةِ بالمريضِ إلى شركةِ التأمينِ الصحيّ ، مثلَ التشخيصاتِ وتطوّراتِ العلاجِ والأدويةِ الموصوفةِ ونتائجِ التحاليلِ المخبريَّة . وتساعدُ هذه المعلوماتُ شركةَ التأمينِ الصحيّ على تقييمِ ضرورةِ وملاءمةِ الرعايةِ الطبيَّةِ واستردادِ الخدماتِ المناسبة .

2ـ بياناتُ التسويةِ الماليَّة : ترسلُ المؤسَّسةُ الطبيَّةُ بياناتِ التسويةِ الماليَّةِ إلى شركةِ التأمينِ الصحي ، مثلَ الخدماتِ المقدّمةِ وأسعارِ الرسومِ ومدّةِ العلاج ، و تساهمُ هذه المعلوماتُ في التسويةِ الصحيحةِ بينَ المؤسَّسةِ الطبيَّةِ وشركةِ التأمينِ الصحّي وتمكّنُ استردادَ التكاليفِ بشكلٍ سليمٍ .

3ـ أمانُ البياناتِ وحمايةُ الخصوصيَّةِ : يخضعُ تبادلُ البياناتِ بينَ شركاتِ التأمينِ الصحيّ والمؤسَّساتِ الطبيَّةِ لتدابيرِ أمانٍ وحمايةٍ صارمةٍ ، و من المهمّ ضمانُ أنَّ البياناتِ المرسلةَ محميَّةٌ بشكلٍ مناسبٍ لضمانِ سريَّةِ وسلامةِ المعلومات .

4ـ موافقةُ المريضِ : عادةً ما تُنفّذُ عمليَّةُ تبادلِ البياناتِ بينَ شركاتِ التأمينِ الصحيّ والمؤسَّساتِ الطبيَّةِ بناءً على موافقةِ المريضِ ، و يوافقُ المريضُ على إفشاءِ معلوماته الطبيَّةِ وبياناتِ التسويةِ الماليَّةِ لشركةِ التأمينِ الصحيّ لتمكينِ تقديمِ الرعايةِ الصحيَّةِ المناسبةِ واستردادِ التكاليف .

يأخذُ تبادلُ البياناتِ بينَ شركاتِ التأمينِ الصحيّ والمؤسَّساتِ الطبيَّةِ دوراً هامَّاً في تنسيقِ الرعايةِ الصحيَّةِ والتسويةِ الصحيحةِ للخدماتِ المقدّمةِ ، و يسهمُ في تسهيلِ التواصلِ والتعاونِ الفعَّالِ بينَ الأطرافِ المعنيَّةِ ويعزّزُ جودةَ وفعاليَّةَ الرعايةِ الصحيَّةِ .

حظر استخدام بيانات المرضى :

يشيرُ حظرُ استخدامِ بياناتِ المرضى إلى إجراءٍ يُتَّخذُ لتقييدِ أو منعِ الوصولِ إلى معلوماتِ أو بياناتِ المرضى ، و يتمُّ ذلكَ عادةً لأسبابِ حمايةِ الخصوصيَّةِ أو الامتثالِ للقوانينِ والتشريعاتِ القانونيَّةِ والمتطلَّباتِ التنظيميَّةِ الأخرى ، و في سياقِ الرعايةِ الصحيَّةِ ، يمكنُ أنْ يكونَ حظرُ استخدامِ بياناتِ المرضى ذا أهميَّةٍ كبيرةٍ فيما يلي :

1ـ حظرُ حقوقِ الوصولِ : قد يكونُ من الضروريّ حظرُ وصولِ بعضِ الأشخاصِ أو مجموعاتِ المستخدمينَ إلى بعضِ معلوماتِ المرضى ، و يمكنُ أنْ تشملَ هذه المعلوماتُ بياناتٍ طبيَّة حسَّاسة تخصُّ مجموعةً محدودةً من الأفرادِ ، مثلَ المعلوماتِ النفسيَّةِ أو السريَّةِ .

2ـ حظرُ الوصولِ بناءً على الموافقةِ أو سحبِ الإذن : إذ يحقُّ للمريضِ حظرُ الوصولِ إلى بياناتِه أو سحبِ موافقتِه على استخدامِ بياناتِه أو مشاركتِها في أيّ وقت ، و في هذهِ الحالةِ تُحظّرُ البياناتُ المعنيَّةُ بحمايتُها من الوصولِ غير المصرَّحِ به.

3ـ حظرُ الوصولِ بسببِ الفقدانِ أو السرقة : في حالةِ فقدانِ أو سرقةِ وسائطِ التخزينِ الَّتي تحتوي على بياناتِ المرضى ، قد يكونُ من الضروريّ حظرُ البياناتِ المتأثّرةِ فوراً لمنعِ أيّ سوءِ استخدامٍ محتملٍ أو الوصولِ غيرِ المصرَّحِ به .

4ـ حظرُ الوصولِ بعد الحذفِ أو التدميرِ : عندَ حذفِ بياناتِ المرضى وفقاً لفتراتِ الاحتفاظِ القانونيَّة المعمولِ بها أو تدميرِها ، يجبُ حظرُها مسبقاً لضمانِ عدمِ استخدامِها أو الوصولِ إليها بشكلٍ غيرِ مقصودٍ أو متعمَّد .

و حظرُ استخدامِ بياناتِ المرضى هو آليَّةُ حمايةٍ هامَّةٍ تهدفُ إلى ضمانِ سريَّةِ ونزاهةِ المعلوماتِ الشخصيَّةِ للمرضى ، و يضمنُ أنْ يكونَ للأشخاصِ المخوَّلينَ فقط الوصولُ إلى البياناتِ وأنْ تُعاملَ وفقاً للقوانينِ والتشريعاتِ الخاصّةِ بحمايةِ البياناتِ ، و يتطلَّبُ حظرُ استخدامِ بياناتِ المرضى الامتثالَ للسياساتِ والإجراءاتِ الصارمةِ للحفاظِ على الخصوصيَّةِ والحمايةِ الأمنيَّةِ لهذهِ البيانات .

يشيرُ حذفُ بياناتِ المرضى إلى عمليَّةِ إزالةِ معلوماتِ الهويَّةِ الشخصيَّةِ للمرضى من نظامِ البياناتِ أو التسجيلِ بشكلٍ دائمٍ ، و يُعمَلُ بهذا عادةً لضمانِ الخصوصيَّةِ وحمايةِ البياناتِ الشخصيَّةِ للمرضى وضمانِ عدمِ استخدامِ البياناتِ أو الوصولَ إليها بعدَ ذلك ، و عندَ حذفِ بياناتِ المرضى هناكَ بعضُ الجوانبِ المهمَّةِ الَّتي يجبُ مراعاتها :

1ـ الأسسُ القانونيَّةُ : يجب أن تُحذَفَ بياناتُ المرضى وفقاً للقوانينِ واللوائحِ المعمولِ بها في مجالِ حمايةِ البياناتِ ، ويشملُ ذلكَ بشكلٍ خاص أحكامَ الاحتفاظِ بالسجلّاتِ الطبيَّةِ والامتثال لفتراتِ الحفظِ والاحتفاظِ بالبياناتِ .

2ـ الإجراءاتُ والتدابيرُ الأمنيَّة : يتطلَّبُ حذفُ بياناتِ المرضى اتّخاذَ إجراءاتٍ وتدابيرَ أمنيَّةٍ محدَّدةٍ لضمانِ حذفِ البياناتِ بشكلٍ نهائي وغيرِ قابلٍ للاسترجادِ ، ويمكنُ أنْ يشملَ ذلك استخدامَ خوارزمياتِ الحذفِ الآمنةِ ، أو تدميرَ وسائطِ التخزينِ ، أو استخدامَ برامجِ حذفٍ مخصَّصة .

3ـ التوثيقُ : من المهمّ توثيقُ عمليَّةِ حذفِ بياناتِ المرضى ، بما في ذلكَ وقتَ الحذفِ ، وفئاتَ البياناتِ المتأثّرةِ ، والشخصَ أو المؤسَّسةَ المسؤولةَ عن ذلكَ ، و يهدفُ ذلكَ إلى ضمانِ قابليَّةِ تتبّع وشفافيَّةِ عمليَّةِ الحذف .

4ـ حقوقُ حمايةِ البياناتِ للمرضى : إذ يحقُّ للمرضى طلبُ حذفِ بياناتِهم الشخصيَّةِ ، ما لم تكن هناكَ أسبابٌ قانونيَّةٌ للاحتفاظِ بها ، و في مثلِ هذه الحالاتِ يجبُ حذفُ البياناتِ فوراً ، ما لم تكنْ هناكَ واجباتٌ قانونيَّةٌ للاحتفاظِ بالبياناتِ أو التزاماتٌ قانونيَّةٌ أخرى .

و حذفُ بياناتِ المرضى هو جانبٌ مهمٌّ في حمايةِ البياناتِ الشخصيَّةِ في مجالِ الرعايةِ الصحيَّةِ ، حيثُ يساهمُ في ضمانِ سريَّةِ وخصوصيَّةِ المرضى ، و يساعدُ على ضمانِ استخدامِ البياناتِ فقط للأغراضِ المخصَّصةِ لها وأنَّها لا تكونُ متاحةً إلَّا المصرَّحَ بها منها .

الملفُ الصحيُّ الإلكترونيُّ

الملفُ الصحيُّ الإلكترونيُّ هو منصَّةٌ رقميَّةٌ يمكنُ للمؤمَّنِ عليهِم الاحتفاظُ ببياناتِهم الصحيَّةِ وإدارتِها، و يمكنُ للأطبَّاءِ والمستشفياتِ والأخصائيّينَ والصيدلياتِ فقط الاطلاعُ على هذهِ المعلوماتِ أو حفظِها بشكلٍ ذاتي إذا وعدَ المريضُ بذلك ، بالنسبةِ للشركاتِ التأمينيَّةِ الصحيَّةِ ، ليسَ لديهِم حقُّ الاطلاعِ على هذه البياناتِ وفقاً لوزارةِ الصّحةِ الاتّحادية .

و يمكنُ للمؤمَّنِ عليهِم تخزينُ جميعُ بياناتِ المرضى هناك ، مثلَ التشخيصاتِ والتحاليلِ وإجراءاتِ العلاجِ والفحوصاتِ والمراسلاتِ الطبيَّة.

يحصلُ الأطبَّاءُ ومقدّمو الخدماتِ الصحيَّةِ الآخرونَ على نظرةٍ أفضلَ على تاريخِ المرضى بسببِ تجميعِ البياناتِ في مكانٍ واحدٍ ، وهذا يُسهّلُ عليهِم اختيارَ طريقةِ العلاجِ المناسبةِ ، بالإضافةِ إلى ذلكَ يمكنُ لأطرافِ الرعايةِ الصحيَّةِ تبادلُ المعلوماتِ بينَهُم بشكلٍ أفضل .

و ابتداءً من 1 يناير 2021م ، يُوفَّرُ ملفُ المريضِ الإلكتروني (ePA) الاختياري لجميعِ المؤمَّنِ عليهِم ضمنَ نظامِ التأمينِ الصحيّ القانوني ، و تحصلُ هذهِ الملفاتُ من شركاتِ التأمينِ الصحيّ ، وفي هذا الملفِ تُخزَّنُ معلوماتٌ مثل :

-التشخيصات والنتائج الطبيَّة .

-الأمراض المزمنة السابقة .

-الحساسيَّة للأدوية .

-التطعيمات .

-جدول الأدوية ، والعلاجات ، وإجراءاتِ العلاج .

-المراسلاتُ الطبيَّةُ .

-نتائجُ فحوصَ الدم .

-صورُ الأشعّة .

-دفترُ التطعيمات ، كشوف الأسنان ، ملف الأمهات ، كشوفات الفحوص الطبيَّةِ للأطفال (ابتداءً من عام 2022م).

و في الوقتِ الحالي ، تقدّمُ شركاتُ التأمينِ الصحيّ الملفَ الطبيَّ الإلكترونيَّ مع تطبيقٍ للمريضِ ، و يمكنُ للمريضِ من خلالِ هذا التطبيقِ تحميلُ المستنداتِ ، ورسائلِ الأطبَّاءِ ، والتقاريرَ الطبيَّةَ ، وغيرها. و يعني ذلكَ أنَّ المريضَ وحدَهُ يقرّرُ البياناتِ الَّتي ستُخزَّنُ بخصوصِ العلاجِ المعيَّن ، و البياناتِ الَّتي لن تخزّن ، كما يمكنُه حذفُ معلوماتٍ فرديَّةٍ أيضاً .

المريضُ هو الَّذي يقرّرُ ما إذا كانَ الوصولُ إلى المعلوماتِ المتعلّقةِ بالعلاجِ الحاليّ سيكونُ محدوداً أو ممكناً لفترةٍ طويلةٍ من دونِ موافقتِه ، و لا يجوزُ تخزينُ المعلوماتِ أو الاطلاعَ عليها ، و هذا يُعطي المريضَ السيطرةَ الكاملةَ على بياناتِه الصحيَّةِ وحمايةَ خصوصيَّتِه .

و بالتالي ، ليسَ لدى الأطبَّاءِ حقُّ الحكمِ ولا الوصولُ المباشرُ ، وفقط بعدَ موافقةِ المريضِ والتصريحِ الفنيّ يجوزُ لهُم الوصولُ إلى الملفّ الطبيّ الإلكترونيّ للمريضِ .

حتَّى الآن ، كانَ الحصولُ على وصفةٍ طبيَّةٍ في عيادةِ الطبيبِ يتمُّ عن طريقِ الحصولِ على ورقةٍ ورديَّةٍ يُقدّمُها المريضُ في الصيدليَّةِ مقابلَ الأدويةِ ، من المفترضِ أنْ تُستَبدلَ هذه الخطوةُ في المستقبلِ بالوصفةِ الرقميَّةِ ، المعروفةُ أيضاً بالوصفةِ الإلكترونيَّةِ ، ومع ذلك تواجهُ عمليَّةُ التنفيذِ صعوباتٍ حاليَّاً بسببِ التحفّظاتِ المتعلّقةِ بالخصوصيَّةِ والأمان ، و لا يزالُ غيرُ واضحٍ بالضبطِ كيفيَّة استمرارِ عمليَّةِ التنفيذِ في المستقبل .

و من خلالِ رمزQR ، يمكنُ الوصولُ إلى الوصفةِ الطبيَّةِ الرقميَّةِ على الهاتفِ الذكي ، يمكنُ للمرضى بالطريقةِ هذهِ استلامَ الوصفاتِ الطبيَّةِ من عياداتِ الأطبَّاءِ بشكلٍ إلكتروني عبرَ تطبيقِ ، وإدارتها ، وتقديمُهَا في الصيدليّة ، وبالتالي تُبسطُ العمليَّاتُ في العياداتِ الطبيَّةِ والصيدليات ، ويقلّلُ من مواعيدِ الحضورِ للطبيبِ والمسافاتِ المطلوبة ، كما يساعدُ تخزينُ الوصفاتِ الطبيَّةِ إلكترونيَّاً على تحديدِ تداخلاتِ الأدويةِ الموصوفةِ بشكلٍ أسرع .

تُخزَّنُ البياناتُ بشكلٍ مشفّر على خوادمِ البنيةِ التحتيَّةِ للتليماتك (Telematikinfrastruktur - TI) ، حسبَ مؤسَّسة .gematik GmbH تعدُّ التليماتك بنيةً تحتيَّةً افتراضيَّة تسمحُ للأطبَّاءِ بتبادلِ المعلومات، وتكونُ البياناتُ المخزَّنةُ هناكَ قابلةً للاسترجادِ فقط من خلالِ رمزِ الاستجابة السريعة .(QR) ومع ذلك، يتطلَّبُ ضمانُ حمايةِ بياناتِ المرضى اتّخاذَ إجراءاتٍ تقنيَّةٍ وتنظيميَّةٍ مناسبةٍ ، و يجبُ أن تكونَ هذه الإجراءاتُ متوافقةً مع أحدثِ التقنيَّاتِ المتوفّرةِ ويجبُ تحديثُها باستمرار .

تأجَّلَ إدخالُ الوصفِ الإلكترونيّ للمرضى من قِبَل الجمعيَّةِ الطبيَّةِ في غربفالين- ليبه .(KVWL) وذلكَ بسببِ موقفِ المفوَّضِ الاتّحادي لحمايةِ البياناتِ ، حيثُ أعلنَتْ جمعيَّةُ الأطبَّاءِ في 3 نوفمبر 2022 م في دورتموند أنَّها تضطرُّ إلى تأجيلِ العمليَّةِ بناءً على طلبِ المفوَّضِ لحمايةِ البيانات أولريش كلبير (عن حزب الاشتراكي الديمقراطي) ، وقد فرضَ كلبير في سبتمبر 2022م حظر على خططِ استخدامِ بطاقات التأمينِ الصحي للمرضى في الوصفِ الإلكتروني .

حتَّى الآن ، يمكنُ للمرضى الحصولُ على الوصفةِ الطبيَّةِ الإلكترونيَّةِ عبرَ هواتِفهم المحمولةِ أو عن طريقِ طباعتِها ، يتطلَّبُ الحصولُ على التطبيقِ رمز PIN من شركةِ التأمينِ الصحي - الَّذي يمكنُ الحصولُ عليهِ فقط بعدَ التحقّق الشخصيُّ في مكتبِ التأمينِ الصحيّ أو عبرَ البريدِ ، و على ما يبدو يعدُّ

العديدُ من النَّاسِ هذه الإجراءات معقدة وصعبة ، حيثُ قُدّمَتْ طلباتٌ للحصولِ على رمزِ PIN بأعدادٍ قليلةٍ فقط .

الطبُّ عن بُعد :

تندرجُ بياناتُ صحّةِ الأشخاصِ الطبيعيَّة ضمنَ الفئاتِ الخاصَّةِ بالبياناتِ الشخصيَّة وتحمى وفقاً للقوانينِ الخاصَّةِ بحمايةِ البياناتِ ، وليسَ فقط بتنفيذِ قواعدِ الحمايةِ العامَّةِ للبياناتِ .(GDPR) سواءً كانَ التعاملُ مع هذهِ البياناتِ بشكلٍ تقليدي أو تلقائي ، فإنَّ معالجةَ هذه البياناتِ تتطلَّبُ مستوى عالٍ من الحذرِ والتدابير الأمنيَّة .

أُصدِرَ ما يسمَّى بقانونِ الصحة الإلكترونيَّةِ في عامِ 2015م لإنشاءِ إطارٍ قانونيّ للتعاملِ مع بياناتش المرضى في مشاريعِ الطب عن بُعد ، ودخلَ هذا القانونُ حيّزَ التنفيذِ في نفسِ العام (تمَّ تحديثُه في عامي 2016 و 2017م).

يشيرُ الاسمُ الكاملُ "قانونَ الاتّصالِ الرقميّ الآمن والتطبيقاتِ في الرعايةِ الصحيَّةِ وتعديلَ بعضِ القوانين" إلَّا أنَّه لا يوجدُ قانونٌ مستقلٌّ للطبّ عن بُعد ، بل تتماشى قواعدُ مختلفة في هذا المجالِ معاً ، و تهدفُ قوانينُ الصّحةِ الإلكترونيَّةِ إلى تنفيذِ وتطبيقِ تطبيقاتِ الطبّ عن بُعد المختلفة ، و على سبيلِ المثال أصبحَتْ الاستشاراتُ عبرَ الفيديو مسموحاً بها منذُ عام 2017م .

و خاصَّةً عمليَّةُ نقلِ البياناتِ تمثّلُ تحدّياً كبيراً أمامَ الأطبَّاءِ ، و يتطلَّبُ التعاملُ مع بياناتِ الصّحةِ الَّتي تحتاجُ إلى حمايةٍ خاصَّةٍ و بنيةٍ تحتيَّةٍ آمنةٍ تمنعُ بالتأكيدِ الوصولَ إليها من قِبَلِ جهاتٍ غيرِ مخوَّلة ، وهذا لا يشملُ فقط تأمينَ الاتّصالاتِ عبرَ الانترنت ، وعندَ إجراءِ الاستشاراتِ عبرَ الفيديو أو التشاورَ مع طبيبٍ آخر ، يجبُ ضمانُ أنَّ الاتّصالَ الهاتفيَّ أيضاً لا يمكنُ الاستماعُ إليه من قِبَل غيرِ المخوَّلين .

علاوةً على ذلك ، يجبُ توخّي الحذرِ بشكلٍ خاص عندَ إرسالِ نتائجِ الفحوصاتِ أو الصورِ الطبيَّةِ للأشخاصِ المخوّلينَ بذلك ، إذ يجبُ أنْ يكونَ من المؤكّدِ تماماً أنَّ الشخصَ الَّذي يطلبُ البياناتِ هو شخصٌ مخوَّلٌ له الوصولُ لهذه البياناتِ وله حقُّ الاطلاعِ ، و قد تكونُ عمليَّةُ تأمينِ التواصلِ صعبةً بشكلٍ خاص عندَ استخدامِ البريدِ الإلكتروني أو الهاتف ، وتكونُ التدابيرُ التقنيَّةُ الَّتي يجبُ اتّخاذها بسببِ الفئاتِ الخاصَّةِ للبياناتِ هذه أكثرَ تعقيداً (من التّحكم في الوصولِ لنقلِ البياناتِ إلى شركاتِ التأمينِ الصحيّ وما إلى ذلك).

يُستخدَمُ الذكاءُ الاصطناعيُّ بالفعلِ في مجالِ الطبّ ويعودُ هذا إلى وقتٍ قبلَ إصدار .DSGVO على سبيلِ المثال ، و في نهايةِ عام 2019م ، أشارَ البروفيسور الدكتور /هيساكي ماكيموتو/ في دراسةٍ إلى أنَّ الذكاءَ الاصطناعيَّ يمكنُه التعرّفُ على الإصاباتِ بالأنسجةِ القلبيَّةِ من خلالِ قراءةِ تخطيطِ القلب - وحسبَ ما أفادَ ماكيموتو ، يعملُ الذكاءُ الاصطناعيُّ بهذهِ المهمَّةِ بشكلٍ أفضلٍ حتَّى من الأطبَّاء القلبيّين. وتتنوَّعُ إمكانياتُ استخدامِ الذكاءِ الاصطناعيّ في المجالِ الطبيّ بشكلٍ كبيرٍ : من تحليلِ الصورِ لاكتشافِ الأورامِ ، إلى المستشفياتِ المساعدةِ بالروبوت ، وصولاً إلى اتّخاذِ القراراتِ السريريَّةِ أو استخدامِ أطرافٍ صناعيَّةٍ ذكيَّةٍ .

تتطلَّبُ معالجةُ هذه البياناتِ الشخصيَّةِ الَّتي تتعلَّقُ بالذكاءِ الاصطناعيّ اتّباعَ مبادئ الحمايةِ من البيانات، والَّتي تنصُّ عليها المادَّة /5/ من .DSGVO على سبيلِ المثال ، و يجبُ أن تُعالَجَ البياناتُ الشخصيَّةُ بشكلٍ شفَّافٍ ومفهومٍ للشخصِ المعنيّ بالأمرِ ("شفافية")، وأن تُجمَع لأغراضٍ محدَّدةٍ وواضحةٍ وشرعيَّةٍ وألَّا تُعالَجَ بأيّ طريقةٍ لا تتّفقُ مع هذه الأغراضِ ("التقييد بالأغراض")، وأن تكونَ مناسبةً وملائمةً للأغراضِ وضروريَّةً للمعالجةِ ("تقليل البيانات")، وأن تُخزَّنَ في شكلٍ يُمكِّن من التعرّفِ على الأشخاصِ المعنيّين بالأمرِ لفترةٍ لا تزيدُ عن الفترةِ المطلوبةِ للأغراضِ الَّتي تُعَالَجُ فيها ("تقييد الاحتفاظ").

يثيرُ بالفعلِ مبدأَ الشفافيَّةِ صعوبةً كبيرةً في الوفاءِ به ، و بسببِ تعقيدِ عمليَّاتِ المعالجةِ ، يكونُ من الصعبِ على المُطَوِر إيجادُ حلٍّ يعتمدُ على الذكاءِ الاصطناعيّ ضمانَ شفافيَّةِ هذهِ المعالجة ، على سبيلِ المثالِ ، لا يمكنُ لمستخدمي ChatGPT معرفةُ كيفيَّةِ معالجةِ البرنامجِ للبياناتِ الشخصيَّةِ الَّتي تُدخَلُ في نافذةِ الدردشة .

وبالإضافةِ إلى ذلك ، يتعارضُ مفهومُ Big Data مع المبادئِ الأخرى المذكورةِ أعلاه لحمايةِ البيانات، و على سبيلِ المثال ، قد يحتاجُ الذكاءُ الاصطناعيُّ إلى التعرّفِ على أنواعٍ مختلفةٍ من الأنسجةِ القلبيَّةِ من خلالِ قراءةِ تخطيطِ القلبِ لتحقيقِ هذا الهدف ، يتمكن الذكاءُ الاصطناعيُّ التعلّمَ من العديدِ من تخطيطاتِ القلب ، و يشيرُ المفهومُ نفسُه إلى أنَّه يجبُ الاستفادةُ من البياناتِ في أكبرِ قدرٍ ممكن ، وهذا يعني أنَّ

البياناتِ تُعالجُ لفترةٍ أطولَ من فترةِ معالجتِها المطلوبةِ بغرضِ التعلّم والتعرفِ على نمط مشكلةٍ أخرى لحمايةِ البياناتِ تكمنُ في العلاقةِ مع الأشخاصِ المعنيّينَ ، و وفقاً للمادَّةِ /12/ وما يلي منDSGVO ، يجبُ إبلاغُ الأشخاصِ المعنيّينَ قبلَ معالجةِ البياناتِ حولَ هويَّةِ المعالجِ والأغراضِ الَّتي تُعالَجُ فيها البياناتُ ، ومع ذلك فإنَّ جمعَ البياناتِ في كثيرٍ من الأحيانِ لا يكونُ شفَّافاً لدرجةِ أنَّهُ في بعضِ الأحيانِ، حتَّى المُصنِّع نفسُه لا يعرفُ إلى أيّ بياناتٍ يُمكنُ للذكاءِ الاصطناعي الوصولُ حاليَّاً، بحيثُ يكونُ من الصعبِ على الأشخاصِ المعنيّينَ تلقّي إخطار.

وبالإضافةِ إلى ذلك ، قد يكونُ حجمُ البياناتِ كبيراً لدرجةِ أنَّهُ يبدو من غيرِ الممكنِ بالفعلِ إبلاغُ كلّ شخصٍ معنيّ ، و في هذا السياقِ، يُصبِحُ مهمَّاً أيضاً ممارسةُ حقوقِ الأشخاصِ المعنيّين ، و من الجديرِ بالذكرِ أنَّهُ يجبُ أنْ تُحذَفَ البياناتُ الشخصيَّةُ الَّتي عالجها من قبل الذكاءُ الاصطناعيُّ وفقاً للمادَّةِ /17/ منDSGVO ، أو كيفَ يمكنُ تقديمُ معلوماتٍ للأشخاصِ المعنيّينَ بخصوصِ هذهِ البيانات.

بالإضافةِ إلى مخاطرِ الذكاءِ الاصطناعيّ ، يجبُ أنْ نأخذَ في الحسبانِ أنَّ بياناتِ الصّحةِ تخضعُ لحمايةٍ خاصَّةٍ بموجبِDSGVO ، نظراً لأنَّها حسَّاسةٌ بشكلٍ خاص ، و ينطبقُ هنا بشكلٍ عام حظرُ معالجةِ البياناتِ ، وتوجدُ استثناءاتٌ وفقاً للمادَّة /9/ الفصل/2/ من DSGVO ، ومن بينِ هذهِ الاستثناءاتِ خاصَّةً الإذنُ المعلنُ عنه ، ومع ذلك تظهرُ مشكلةُ عدمِ الشفافيَّةِ المذكورةِ أعلاه حينئذٍ ، بحيثُ تكونُ المعلوماتُ الَّتي يتلقَّاها الأشخاصُ المعنيّونَ في معظم الأحيان غير كافية، وبالتالي يصبح الإذن مشكلة.

تتطلب المادة /35/ من DSGVO إجراءَ تقييمٍ للمخاطرِ على الحمايةِ من البياناتِ في حالِ كانَ هناكَ نوعٌ من المعالجةِ ، ولا سيما في حالةِ استخدامِ التقنيَّاتِ الجديدة ، نتيجةً لطبيعةِ المعالجةِ ونطاقِها وظروفِها وأغراضِها ، و غالباً ما يجعلُ استخدامُ الذكاءِ الاصطناعيّ مثلَ هذا التقييمِ ضروريَّاً ، ويمكنُ أن يساهمَ هذا التقييمُ بشكلٍ كبيرٍ في تحسينِ الأمانِ في معالجةِ البياناتِ من خلالِ أنظمةِ الذكاءِ الاصطناعيّ (القانونية)، ويمكنُ للمستخدمِ التقييمُ على ضوءِ هذا ما إذا كانَ من الضروريّ الرجوعُ إلى السلطةِ التنظيميَّةِ السابقةِ وفقاً للمادَّةِ /36/ منDSGVO

و علاوةً على ذلك ، يجبُ على مستخدِمي الذكاءِ الاصطناعيّ أن يسعوا لتحقيقِ أقصى درجاتِ الأمانِ من حيثُ البياناتِ ، و من الأفضلِ اتّخاذُ جميعِ التدابيرِ التكنولوجيَّةِ والتنظيميَّةِ الَّلازمةِ لحمايةِ البياناتِ الشخصيَّةِ من الوصولِ غير المصرَّحِ به .

تزدادُ حالاتُ انتهاكِ الخصوصيَّةِ بشكلٍ متزايدٍ وتصبحُ أكثرَ تطوَّراً وتؤثّرُ على جميعِ أنواعِ الشركاتِ،و يمكنُ أن تتعرَّضَ في هذهِ الانتهاكاتِ بياناتٍ طبيَّةٍ وبياناتٍ شخصيَّةٍ ومعلوماتٍ سريَّةٍ للشركاتِ للكشفِ عنها أو سرقتِها أو إساءةِ استخدامِها .

ووفقاً لشركةِ IBM ، أُبلِغَ عن نحو /109,000/ انتهاكٍ للخصوصيَّةِ للسلطاتِ الرقابيَّةِ ، وكانَتْ التكلفة المتوسّطةُ لكلّ حادثٍ نحو /4.35/ مليون دولار أمريكي .

و في وقتٍ قريبٍ، حدث انقطاع آخر للبيانات في شركةT-Mobile ، أثر على نحو 37 مليون عميل ما قبل الدفع وما بعد الدفع، وتم تعريض بياناتهم للخطر.

وعلى مدى السنواتِ الاثني عشرةَ الماضيةِ ، كانَتْ الولاياتُ المتّحدةُ تتصدَّرُ قائمةَ أعلى التكاليفِ لانتهاكِ الخصوصيَّةِ ، و في عامِ 2022م ، بلغَتْ التكاليفُ المتوسّطةُ نحو /9.44/ مليون دولار، وهو أكثرُ من ضعفِ المتوسّطِ العالمي .

كانَ قطَّاعُ الرعايةِ الصحيَّةِ من بينِ الأكثرِ تأثّراً : بلغَتْ التكاليفُ المتوسّطةُ لانتهاكِ الخصوصيَّةِ حوالي /10.1/ مليون دولار، وزادَتْ بنسبةِ 42% منذُ عام 2020م ، وقد احتلَّ قطَّاعُ الرعايةِ الصحيَّةِ المركز الأول لأعلى تكاليفِ متوسّطة لانتهاكِ الخصوصيَّةِ للسنة الثانية عشرةَ على التوالي .

يحدثُ 45% من جميعِ انتهاكاتِ الخصوصيَّةِ في التخزينِ السحابيّ ، وتتراوحُ التكاليفُ المتوسّطةُ لانتهاكِ الخصوصيَّةِ في الشركاتِ الَّتي تستخدمُ سحاباتٍ خاصَّة حوالي 4.24 مليون دولار، بينما تصلُ إلى 5.02 مليون دولار في السحاباتِ العامَّة.

و تزدادُ أهميَّةُ قوانينِ حمايةِ البياناتِ في جميعِ أنحاءِ العالم ، حيثُ تُجمَعُ و تُخزَّنُ و تُعَالَجُ البياناتُ الشخصيَّةُ بشكلٍ واسع ، و في الاتّحادِ الأوروبيّ والولاياتِ المتّحدة ، وُضِعَ GDPR و CCPA في العامِ 2018م و 2020م على التوالي ووُضِعَتْ معاييرٌ عاليةٌ لحقوقِ حمايةِ البيانات.

71%من بلدانِ العالمِ وضعَتْ قوانينَ لحمايةِ البياناتِ والخصوصيَّةِ ، و في الوقتِ نفسِه، لا يوجدُ تشريعٌ في 15% من البلدان، و9% لديها مشروع قانون و5% لا تتوفّرُ لديها بياناتٌ حولَ هذا الموضوع .

يبلغُ إجمالي الغراماتِ المفروضةِ بموجبِ قوانينِ حمايةِ البياناتِ العامَّةِ للمرتبةِ حوالي 56 مليون يورو، ولكن تُعزى نسبةُ 90% تقريباً من هذا المبلغِ إلى غرامةٍ واحدةٍ فقط : وهي أنَّ عقوبةَ الغرامةِ الَّتي فرضّتها السلطةُ الفرنسيَّةُ لحمايةِ البياناتِ CNIL على جوجل بقيمة 50 مليون يورو.

و فيما يتعلّقُ بموقع Amazon.com ، أُدينَتْ الشركةُ بغرامةٍ قدرها 877 مليون دولار أمريكي من قبلِ لوكسمبورج بسببِ انتهاكٍ للحصولِ على معلوماتٍ حسبَ اللوائحِ العامَّةِ لحمايةِ البيانات.

أكثرُ من 60% من الشركاتِ حولَ العالمِ تزيدُ من استثماراتِها في الامتثالِ لقواعدِ حمايةِ البياناتِ نتيجةً للتشريعاتِ مثل GDPR و.CCPA

هل تمَّ تجاوزُ حمايةِ البياناتِ الشخصيَّةِ في أزمة كورونا؟

لا ، إذ تخضع جميعُ البياناتِ الصحيَّةِ للتدابيرِ الصارمةِ في أثناءِ جائحةِ كورونا لأنَّ هذهِ البياناتِ تندرجُ ضمنَ الفئاتِ الخاصَّةِ من البياناتِ الشخصيَّةِ ، و تكونُ الأوامرُ أقلَّ صرامةً فيما يتعلّقُ ببياناتِ العنوان - مثلَ قوائمِ الزوَّارِ في المطاعمِ وما شابه ، ولكن حتَّى هنا يجبُ ألَّا تُستخدَمَ المعلوماتُ في معظمِ الحالاتِ لأغراضٍ غيرِ قانونيَّة .

و على الرغمِ من صرامةِ حمايةِ بياناتِ الصحةِ (الَّتي تندرجُ ضمنَ الفئاتِ الخاصَّة من البياناتِ الشخصيَّة)، يُسمَحُ بشكلٍ واسعٍ بجمعِ البياناتِ في ظلّ جائحةِ كورونا ، يتضمَّنُ ذلكَ معلوماتٍ حولَ ما إذا كانَ هناك إصابة بفيروس SARS-CoV-2 أو تواجد اتّصالٍ مع شخصٍ مصابٍ بالفيروس ، أو إذا عادَ المعنيُّ من منطقةٍ ذاتِ مخاطر ، من يحق له اتّخاذ إجراءات مناسبةٍ للتعامل مع الوباء؟ و ما هي الإجراءاتُ المشروعةُ الَّتي يجوز عملها لتفادي الانتشار الأوسعِ للوباء ؟

- جمعُ ومعالجةُ بياناتِ الصحةِ للموظَّفينَ للسيطرةِ على انتشارِ فيروس كورونا الجديدِ داخلَ الشركات-

- جمعُ ومعالجةُ بياناتِ الصحةِ للضيوفِ والزائرين (أيضاً لأغراضِ إعادةِ البناءِ للسلطات)-

- الكشفُ عن المعلوماتِ المناسبةِ، مثلَ إبلاغِ الأشخاصِ المتّصلين ، إذ يجبُ أن يُكشَفَ عن هويَّةِ المعني هنا فقط إذا كانَ ذلك ضروريَّاً لتحديدِ وإبلاغِ الأشخاصِ المتّصلين بشكلٍ استثنائي .

- جمعُ البياناتِ الشخصيَّةِ من المسافرينَ العائدينَ من مناطقَ ذاتِ مخاطر لتتبّع سلاسلِ العدوى المحتملة.

- نقلُ المعلوماتِ حولَ الإصاباتِ المؤكَّدةِ من قِبلِ المختبراتِ أو الأطبَّاءِ إلى مكاتبِ الصّحةِ (وقد تتضمَّنُ تحديدَ هويَّةِ الشخصِ لتتمكّنَ من تحديدِ الأشخاصِ المتّصلينَ المحتملين) ، و نظراً لأنَّ فيروس كورونا الجديد يُعدُّ حالياً من الأمراضِ الَّتي يجبُ الإبلاغُ عنها ، إذ يجبُ أنْ تُبلِغَ هذه المعلومات حتَّى لو كانت تتضمَّنُ تحديدَ هويَّةِ الشخص.

الدراساتُ السريريّة

في كلّ دراسةٍ سريريَّةٍ ، تُعالَجُ البياناتُ الشخصيَّةُ للمرضى ، بما في ذلكَ المتطوّعين أحياناً ، حتَّى إذا تمَّتْ المساهمةُ في الدراساتِ باستخدامِ بياناتٍ مجهولةٍ ، يجبُ أنْ تُجمعَ البياناتُ الشخصيَّةُ أولاً ثمَّ تُجعَل مجهولةً ، ولذلك يجبُ الالتزامُ بالإطارِ القانونيّ لحمايةِ البياناتِ في كلّ دراسةٍ سريريَّةٍ بشكلٍ عام ، و تعالِجُ الدراساتُ السريريَّةُ الفئاتِ الخاصَّة من البياناتِ المصنَّفةِ في المادَّةِ 9 (1) من لائحةِ حمايةِ البياناتِ العامَّةِ للاتّحادِ الأوروبيّ ، وبخاصَّةٍ البياناتِ الصحيَّة والبياناتِ الجينيَّة ، و تتضمَّنُ معالجةُ هذه البياناتِ بناءً على توجيهاتِ لائحةِ حمايةِ البياناتِ العامَّة دائماً مخاطرَ كبيرة لحقوقِ الأفرادِ المتأثّرينَ وحريَّاتِهم الأساسيَّة .

و في دراساتِ المراجعةِ ، تُجمَعُ البياناتُ حتَّى قبلَ بدءِ الدراسةِ ، حيثُ تُستَخدمُ بياناتُ المرضى من العلاجاتِ الَّتي حدثَت في الماضي ، ومع ذلك تُجمَعُ بياناتُ المرضى في منشآتِ الرعايةِ الصحيَّةِ لأغراضِ الرعايةِ الصحيَّةِ للمرضى ، وليسَ لاستخدامِ البياناتِ للدراسة ، و لذلكَ يُعرَّفُ هذا الاستخدامُ بـ "استخدام ثانوي" للبياناتِ ؛ حيثُ كانَ الهدفُ الأساسيُّ لمعالجةِ البياناتِ هو رعايةُ المرضى ، وفي هذا التغييرِ الهدفيّ يكمنُ بطبيعتِه مخاطرُ إضافيَّةٌ لبياناتِ المرضى بالفعلِ في الاستخدامِ الإضافيّ بذاتِه .

لذلك، من الضروريّ في الدراساتِ السريريَّةِ الالتزامُ بالإرشاداتِ القانونيَّةِ لحمايةِ البياناتِ ، ومن أجلِ تبسيطِ التعاملِ مع التوجيهاتِ الناجمةِ عن قوانينِ حمايةِ البياناتِ في أثناءِ تنفيذِ الدراساتِ السريريَّةِ، أعدَّتْ جمعيةُ المعلوماتِ الطبيَّة والإحصاءِ الوبائيّ في ألمانيا والجمعيةُ الألمانيَّةُ لحمايةِ البياناتِ والأمانِ وثيقةَ عملٍ من 90 صفحة تساعدُ في هذا الموضوع .

إذ تلعبُ حمايةُ البياناتِ دوراً حاسماً في تنفيذِ الدراساتِ السريريَّةِ ، حيثُ تُعالَجُ البياناتُ الشخصيَّةُ للمرضى في هذه الدراساتِ ، تعاونَتْ الجمعيَّةُ الألمانيَّةُ لمعلوماتِ الطبّ الحيويّ والإحصاءِ والوبائياتِ مع المجموعة العمليَّةِ "حماية البيانات وأمان تقنية المعلومات في مجال الرعاية الصحية" بالتعاونِ لإنشاءِ إرشاداتٍ وتوصياتٍ لحمايةِ البياناتِ في الدراساتِ السريريَّة .

تهدفُ هذه الإرشاداتُ إلى ضمانِ الامتثالِ لسياساتِ الخصوصيَّةِ ، والحفاظِ على خصوصيَّةِ الأفرادِ المعنيّينَ في أثناءِ الدراسةِ ، وبشكلٍ خاص يجبُ الالتزامُ بمبادئِ حمايةِ البياناتِ المنصوصِ عليها في لائحةِ حمايةِ البياناتِ العامَّةِ الأوروبيَّةِ (GDPR) عندَ معالجةِ البياناتِ الشخصيَّةِ ، و يتضمَّنُ ذلك الالتزامَ بالشفافيَّة ، وتقييدَ البياناتِ بأغراضٍ محدَّدةٍ وواضحةٍ ومشروعةٍ، والاكتفاءَ بالحدّ الأدنى من البياناتِ اللازمةِ لأغراضِ المعالجة ، وتقييد مدَّةِ تخزينِ البيانات.

و نظراً لأنَّ الدراساتِ السريريَّة غالباً ما تعالجُ بياناتِ فئاتٍ خاصَّةٍ من البيانات ، مثلَ بياناتِ الصّحةِ أو البياناتِ الجينيَّةِ ، فإنَّ معالجةَ هذه البياناتِ تنطوي على مخاطرَ كبيرةٍ لحقوقِ وحريَّاتِ الأفرادِ المعنيّين. لذلكَ من الضروريّ أنْ يقومَ مشغّلو الدراساتِ باتّخاذِ التدابيرِ التقنيَّةِ والتنظيميَّةِ المناسبةِ لضمانِ سلامةِ البياناتِ والامتثالَ لمتطلَّباتِ حمايةِ البيانات.

يهدفُ التعاونُ بينَ الجمعيَّةِ الألمانيَّةِ لمعلوماتِ الطبّ الحيوي والإحصاءِ والوبائيَّاتِ ومجموعةِ العمل "حماية البيانات وأمان تقنية المعلومات في مجال الرعاية الصحية" إلى تسهيلِ التعاملِ مع متطلَّباتِ حمايةِ البياناتِ في الدراساتِ السريريَّةِ ودعمِ الباحثينَ ومشغّلي الدراساتِ في الامتثالِ للمتطلَّباتِ الخاصَّةِ بحمايةِ البياناتِ ، و تهدفُ الإرشاداتُ والتوصياتُ الَّتي أُعدَّتْ لتقديمِ مساعدةٍ عمليَّةٍ ، وإظهارِ الخطواتِ الَّلازمةِ لضمانِ حمايةِ البياناتِ في الدراساتِ السريريَّةِ .

أنظمةُ المعلومات

يعدُّ نظامُ المعلوماتِ هيكلاً أو منصّةً طوّرَتْ لجمعِ وتنظيمِ وتخزينِ ومعالجةِ وإدارةِ البيانات ، يتألَّفُ من مجموعةٍ من الأجهزةِ والبرمجياتِ والشبكاتِ وقواعدِ البياناتِ والإجراءاتِ الَّتي تعملُ سويَّاً لتوليدِ المعلوماتِ واستخدامها .

يقومُ نظامُ المعلوماتِ بجمعِ البياناتِ من مصادر مختلفةٍ ، وتنظيمها في شكلٍ منظّم ، وتوفيرها للمستخدمين ، و يمكنُ لهذا النظامِ إدارةُ مختلفِ أنواعِ المعلوماتِ ، مثلَ معلوماتِ العملاء ، والبياناتِ الماليَّة ، والسجلَّاتِ الطبيَّة ، أو أيَّ بياناتٍ أخرى ذاتِ صلةٍ بنطاقِ التطبيقِ المحدّد .

تُستَخدمُ نظمُ المعلوماتِ لتسهيلِ الوصولِ إلى المعلومات ، ودعمِ تبادلِ المعلوماتِ ، وتحسينِ كفاءةِ العمليَّاتِ ، واتّخاذ القراراتِ المستنيرةِ ، و يمكنُ استخدامُها في مجموعةٍ متنوّعةٍ من الصناعاتِ والقطَّاعاتِ ، مثلَ الرعايةِ الصحيَّةِ ، والتعليم ، والأعمال التجاريَّة ، والجهاتِ الحكوميَّة ، وغيرها الكثير.

و الأمثلةُ على نظمِ المعلوماتِ تشملُ قواعدَ بياناتِ العملاء ، ونظمَ تخطيطِ مواردِ المؤسَّساتِ(ERP) ، ونظمَ إدارةِ المحتوى (CMS) ، وسجلَّاتِ المرضى الإلكترونيَّة(EPA) ، ونظمَ المحاسبةِ الماليَّة ، وغيرها الكثير ، و تلعبُ هذه الأنظمةُ دوراً هامَّاً في إدارةِ المعلوماتِ بشكلٍ فعَّال ، وتأتي بتوفيرِ العمليَّاتِ التلقائيَّة ، ودعمِ عمليَّةِ اتّخاذِ القرار ، وتحسينِ الأداء.

تُستخدَمُ أنظمةُ المعلوماتِ في الرعايةِ الصحيَّةِ بطرائقَ متعدّدةٍ لدعمِ إدارةِ البياناتِ الطبيَّةِ والمعلومات. وفيما يلي بعضُ التطبيقاتِ الشائعةِ لأنظمةِ المعلوماتِ في الرعاية الصحيَّة :

1ـ السجلَّاتُ الطبيَّةُ الإلكترونيَّة : تتيحُ أنظمةُ المعلوماتِ الإلكترونيَّةِ تجميعَ وتخزينَ وإدارةَ بياناتِ المرضى الإلكترونية ، و تشملُ هذه المعلوماتُ الطبيَّةُ التشخيصاتِ وسجلَّاتِ العلاجِ وخططَ الدواء ونتائج الفحوصاتِ الطبيَّة ، تمكّنُ السجلَّاتُ الطبيَّةُ الإلكترونيَّةُ الوصولَ السريعَ والآمنَ إلى بياناتِ المرضى ، سواءً للأطبَّاءِ أو العاملينَ الطبيّين الآخرين .

2ـ أنظمةُ معلوماتِ المستشفى : تدعمُ أنظمةُ معلوماتِ المستشفى إدارةَ المعلوماتِ وتبادلها في المستشفياتِ، و تشملُ وظائفها إدارةَ المرضى وجدولةَ المواعيدِ وإدارةَ الأدويةِ ونتائجَ الفحوصاتِ والتسويةَ الماليَّة ، و تساعدُ هذه الأنظمةُ على تنظيمِ الموارِدِ والخدماتِ في المستشفياتِ بشكلٍ منسّق.

3ـ أنظمةُ معلوماتِ التصويرِ الطبي : تُستخدَمُ في أقسامِ التصويرِ الطبيّ لدعمِ عمليَّةِ جدولةِ المواعيدِ والتصوير، وتقييمِ النتائجِ ، وإعدادِ التقارير ، و تمكّنُ من إدارةِ فحوصاتِ التصويرِ الطبيّ بكفاءةٍ وتيسيرِ التواصلِ بينَ الأطبَّاءِ المُشرفينَ والفنيّين والعاملينَ الآخرين .

4ـ أنظمةُ معلوماتِ المختبر: تُستخدَمُ في المختبراتِ لإدارةِ عمليَّاتِ الفحوصاتِ الطبيَّة ، بما في ذلكَ إدارةَ العيِّناتِ ، وتنفيذَ الاختباراتِ ، وتبادلَ النتائجِ ، وضمانَ الجودةِ ، و تساهمُ في معالجةِ العيِّناتِ المختبريَّةِ بدقّةٍ وكفاءةٍ وتوثيق نتائجِ الاختبارات.

5ـ أنظمة الرعايةِ الصحيَّةِ عن بُعد: تُتيحُ للمرضى المراقبةَ والاستشارةَ عن بُعد ، تُستخدَمُ تقنيّاتٌ مثلَ مكالماتِ الفيديو وأجهزةِ القياسِ عن بُعد ، ومنصّاتِ الاتّصالِ عبرَ الانترنت لتوفيرِ الرعايةِ الطبيَّةِ عن بُعد.

6ـ البواباتُ الصحيَّةُ وبوابَّاتُ المرضى : توفّرُ هذه المنصّاتُ عبرَ الانترنت وصولاً للمرضى إلى بياناتِهم الصحيَّةِ الشخصيَّةِ ، وجدولةَ المواعيدِ والحصولَ على معلوماتٍ طبيَّة ، والتواصلَ مع الأطبَّاء ، و تعزّز ُمشاركةَ المرضى ، وتدعمُ عمليَّةَ اتّخاذِ القرارِ المُشتركِ في الرعاية الطبيَّة .

تساهمُ هذه الأنظمةُ في تحسينِ رعايةِ المرضى وكفاءةِ العمليَّاتِ وأمانِ البياناتِ الطبيَّةِ وتعزيزِ التعاونش بينَ الجهاتِ المختلفةِ في مجالِ الرعايةِ الصحيَّةِ ، و توفّرُ وصولاً سريعاً وآمناً إلى المعلوماتِ ذاتِ الصلةِ، وتدعمُ اتّخاذَ القراراتِ السريريَّةِ ، وتحسينَ جودةِ الرعايةِ الصحيَّةِ بشكلٍ عام .

تُعرَّفُ مبادئُ الوثائقِ بأنَّها المبادئُ الأساسيَّةُ والتوجيهاتُ الَّتي تُتّبعُ في إعدادِ وإدارةِ وحفظِ الوثائقِ والسجلَّاتِ ، و تهدفُ هذهِ المبادئُ إلى ضمانِ سلامةِ وثوابتِ وقابليَّةِ تتبّعِ وتوفّرِ المعلوماتِ ، فيما يلي شرحٌ لبعضِ المبادئِ الوثائقيَّة الهامَّة :

1ـ الاكتمال : يجبُ أنْ تكونَ الوثائقُ كاملةً وتحتوي على جميعِ المعلوماتِ ذاتِ الصلةِ الَّتي تخدمُ الغرضَ المقصودَ والسياق ، و يجبُ ألَّا تفتقرَ الوثائقُ إلى معلوماتٍ هامَّةٍ أو يُتَغاضَى عنْها عمداً.

2ـ الصّحةُ : يجبُ أنْ تكونَ الوثائقُ صحيحةً ودقيقةً ، و يجبُ تمثيلُ جميعِ المعلوماتِ بدقّةٍ وعدمِ تقديمِ معلوماتٍ مضلّلةٍ أو خاطئة ، و من المهمّ أنْ تكونَ المعلوماتُ موثوقةً .

3ـ التناسق: يجبُ أنْ تكونَ الوثائقُ متّسقةً فيما يتعلَّقُ بالتنسيقِ والمصطلحاتِ والهيكلِ ، لضمانِ التواصلِ المتّسقِ والواضحِ ، و يُسهّلُ هذا الأمرُ قراءةَ الوثائقِ وتبادلَها وتفسيرَها .

4ـ قابليَّةُ التتبّع : يجبُ أنْ يكونَ من الممكنِ تتبّعُ عمليَّةِ إعدادِ الوثيقةِ وتتبّعُ التغييراتِ أو التحديثاتِ ، و منَ المهمّ توثيقُ وقتِ ومؤلّفِ ونوعِ التغييراتِ لضمانِ المسؤوليَّةِ وقابليَّةِ التتبّع .

5ـ السريَّةُ وحمايةُ البيانات: يجبُ معاملةُ الوثائقِ بسريَّةٍ خاصَّةٍ عندما تتضمَّنُ بياناتٍ حسَّاسةٍ أو شخصيَّة، و من المهمّ اتّخاذُ تدابيرَ أمنيَّةٍ مناسبةٍ لضمانِ حمايةِ المعلوماتِ ومنعِ الوصولِ غيرِ المصرَّحِ به .

6ـ الاحتفاظُ والأرشفةُ : يجبُ الاحتفاظُ بالوثائقِ وفقاً للسياساتِ والتوجيهاتِ والقوانينِ المعمولِ بها، و يضمنُ هذا الأمرُ إبقاءَ الوثائقِ متاحةً وقابلةً للقراءةِ على مدى فترة زمنيَّةٍ مناسبة .

يعدُّ تطبيقُ مبادئِ الوثائقِ في مجالِ الرعايةِ الصحيَّةِ ذا أهميَّةٍ كبيرةٍ ، حيثُ يضمنونَ جودةً وثباتاً وقابليَّةً التتبّعُ للسجلّاتِ الطبيَّةِ وبياناتِ المرضى وغيرها من الوثائقِ ذاتِ الصلةِ ، ويساعدُ هذا في ضمانِ تقديمِ رعايةٍ آمنةٍ وموثوقةٍ للمرضى والامتثال للمتطلَّباتِ القانونيَّة .

أنظمةُ الأرشفةِ في الرعايةِ الصحيَّةِ هي نظمٌ وعملّياتٌ مخصَّصةٌ طُوّرَتْ لضمانِ الاحتفاظِ بسجلّاتِ المرضى والمستنداتِ الطبيَّةِ وإدارتِها والوصولِ إليها على المدى الطويل ، و تهدفُ إلى الاحتفاظِ بالمعلوماتِ على مدارِ فترةٍ طويلةٍ لتلبيةِ المتطلّباتِ القانونيَّةِ والتنظيميَّةِ والسريريَّةِ ، و فيما يلي بعضُ السّماتِ الرئيسيَّةِ لأنظمةِ الأرشفةِ في الرعايةِ الصحيَّة :

1ـ الأرشفةُ على المدى الطويلِ : تتيحُ أنظمةُ الأرشفةِ الاحتفاظَ بسجلّاتِ المرضى ، والوثائقَ الطبيَّةَ بشكلٍ آمنٍ ودائم على مدى فترةٍ طويلة ، و يشملُ ذلكَ البياناتِ الإلكترونيَّةِ مثلَ سجلّاتِ المرضى الإلكترونيَّة ، بالإضافةِ إلى الوثائقِ الفيزيائيَّةِ مثلَ الملفّاتِ الورقيَّةِ أو الصورَ الشعاعيَّة .

2ـ سلامةُ البيانات : تضمنُ أنظمةُ الأرشفةِ سلامةَ البياناتِ المخزّنةِ ، تُستخدَمُ آلياتٌ لضمانِ حمايةِ البياناتِ من الفقدانِ أو التلفِ أو التلاعبِ غيرِ المصرَّحِ به ، وتشملُ هذه الآلياتُ إجراءَ نسخٍ احتياطيَّةٍ وتشفيرَ البياناتِ وفحصِ سلامةِ البيانات .

3ـ التحكمُ في الوصولِ : تتيحُ أنظمةُ الأرشفةِ التحكمَ في الوصولِ إلى البياناتِ المخزّنة ، و تنفيذَ تدابير أمنيَّةٍ مثلَ التوثيقِ والتصريحِ ووظائفِ تتبّع السجلّاتِ لضمانِ أنْ يتمَّ الوصولُ إلى البياناتِ فقط من قِبلِ المُستخدمين المصرَّحِ لهم .

4ـ وظائفُ البحثِ والاسترجاعِ : توفّرُ أنظمةُ الأرشفةِ وظائفَ بحثٍ واسترجاعٍ قويةً لتسهيلِ الوصولِ إلى المعلوماتِ المخزَّنةِ ، و يمكنُ للمستخدمينَ البحثُ وفقاً لمعاييرَ محددةٍ مثلَ اسمِ المريضِ ، أو التشخيصِ ، أو فترةِ الزمنِ والعثورِ بسرعةٍ على الوثائقِ ذاتِ الصّلة .

5ـ سياساتُ الاحتفاظِ بالسجلّات : تساعدُ أنظمةُ الأرشفةِ على الامتثالِ للمتطلّباتِ القانونيَّةِ والتنظيميَّةِ الاحتفاظَ بسجلّاتِ المرضى ، و تدعمُ تنفيذَ سياساتِ الاحتفاظِ بالسجلّاتِ وتمكّنُ من حذفِ البياناتِ تلقائيّاً بعدَ انتهاءِ فترةِ الاحتفاظِ المحدَّدة .

6ـ التكاملُ مع أنظمةٍ أخرى : غالباً ما تُدمَجُ أنظمةُ الأرشفةِ في البنيةِ التحتيَّةِ لتقنيَّةِ المعلوماتِ الأوسع في قطّاعِ الرعايةِ الصحيَّةِ ، و يمكنُ أنْ تتّصلَ بسجلّاتِ المرضى الإلكترونيَّةِ وأنظمةِ معلوماتِ المستشفى وأنظمةِ معلوماتِ المختبراتِ ، وأنظمةٍ أخرى ذاتِ صلةٍ لتسهيلِ تبادلِ المعلوماتِ بسلاسة .

و يعدُّ تنفيذُ نظامِ أرشفةٍ فعَّالٍ في الرعايةِ الصحيَّةِ أمراً بالغَ الأهميَّةِ لضمانِ الاحتفاظِ بسجلَّاتِ المرضى على المدى الطويلِ والوصولَ الآمنَ إليها ، و يدعمُ سلامةَ البياناتِ ويحمي سريَّةَ المعلوماتِ ويتيحُ إدارةً فعَّالةً لبياناتِ المرضى على مرّ الزمن .

السجلُّ الطبيُّ الإلكترونيُّ هو نسخةٌ رقميَّةٌ من السجلّ الورقيّ التقليدي للمريض ، و يحتوي على معلوماتٍ شاملةٍ حولَ التاريخِ الطبيّ للمريضِ ، بما في ذلكَ التشخيصات ، والعلاجات ، والأدويةَ المُستخدَمة، ونتائجَ الفحوصاتِ المخبريَّة ، وبياناتِ الصورِ الطبيَّةِ ، وغيرها من المعلوماتِ ذاتِ الصلة ، و يُخزَّنُ السجلُّ الطبيُّ الإلكترونيُّ في شكلٍ إلكتروني ، ويمكنُ الوصولُ إليهِ من قبلِ الفرقِ الطبيَّةِ المؤهلةِ عبرَ أنظمةٍ ومنصّاتٍ تقنيَّة المعلوماتِ المختلفة.

و يتمتَّعُ السجلُّ الطبيُّ الإلكترونيُّ بعدّةِ مزايا مقارنةً بالسجلِ الورقيّ التقليدي ، ومن بينها :

1ـ سهولةُ الوصول : يتيحُ السجلُّ الطبيُّ الإلكترونيُّ الوصولَ السريعَ والسهلَ إلى بياناتِ المرضى من مختلفِ المرافقِ الطبيَّة ، و يمكنُ للأطبَّاءِ والفرقِ الطبيَّةِ الأخرى الوصولَ إلى المعلوماتِ بشكلٍ مباشرٍ تقريباً ، ممَّا يسهمُ في تحسينِ تنسيقِ الرعايةِ الصحيَّة .

2ـ تبادلُ البيانات : بفضلِ الطبيعةِ الإلكترونيَّةِ للسجلّ الطبيّ الإلكترونيّ ، و يمكنُ تبادلُ بياناتِ المرضى بسهولةٍ بينَ المرافقِ الطبيَّةِ المختلفة ، و يسهلُ هذا التعاونُ وتنسيقُ العلاجِ بينَ الأطبَّاءِ المختلفينَ والمستشفياتِ والمختبراتِ والمرافقِ الأخرى .

3ـ الدقةُ والاكتماليَّة : يتيحُ السجلُّ الطبيُّ الإلكترونيُّ تحديثاً مستمرَّاً لبياناتِ المرضى ، و يمكنُ إضافةُ المعلوماتِ الجديدة ، مثلَ التشخيصاتِ أو نتائجِ الفحوصاتِ بسرعةٍ ، ويمكنُ توثيقُ التغييراتِ في العلاجِ بشكلٍ فعَّالٍ ، وبذلكَ يتأكَّدُ من أنَّ المعلوماتِ في السجل الطبي الإلكتروني دقيقةٌ ومتكاملة.

4ـ حمايةُ البياناتِ والأمان : يستخدمُ السجلُّ الطبيُّ الإلكترونيُّ تدابيَر أمانٍ صارمةٍ لحمايةِ سريَّةِ وسلامةِ بياناتِ المرضى ، و تتضمَّنُ هذهِ التدابيرُ تقنيَّاتِ التشفير، وضوابطَ الوصولِ ، ووظائفَ مراقبةِ السجلَّات، لضمانِ أن يُوصَلَ إلى المعلوماتِ فقط من قِبلِ الأشخاصِ المخوَّلينَ ، وأنَّ البياناتِ آمنةٌ في أثناءِ النقلِ والتخزين .

تهدفُ تقنيَّةُ السجلّ الطبيّ الإلكترونيّ إلى تحسينِ جودةِ رعايةِ المرضى ، وزيادةِ الكفاءةِ وتسهيلِ تبادلِ المعلومات ، إذ إنَّها توفّرُ منصّةً مركزيَّةً وسهلةَ الوصولِ لتخزينِ وإدارةِ بياناتِ المرضى ، ممَّا يسهمُ في تحسينِ تنسيقِ العلاجِ وتحقيقِ نتائجَ أفضلَ للمرضى.

نظامُ الأرشفةِ والاتّصالُ بالصورِ (PACS) هو نظامٌ معلوماتيٌّ في مجالِ الرعايةِ الصحيَّةِ يُستخدَمُ لتسجيلِ وتخزينِ وإدارةِ وتوزيعِ الصورِ الطبيَّة ، و إنَّه تقنيَّةٌ متقدّمةٌ تتيحُ للمهنيّينَ الطبيّين تسجيلَ وإدارةَ الصورِ الطبيَّةِ مثلَ الأشعّةِ السينيَّةِ وفحوصاتِ الحاسب المقطعي (CT) وصورَ الرنينِ المغناطيسي (MRI)وصورَ الأمواجِ فوق الصوتيَّةِ بتنسيقٍ رقمي.

يتألَّفُ نظامُ PACS من عدَّةِ مكوّنات ، بما في ذلكَ أجهزةَ التصويرِ الطبيّ مثلَ آلاتِ الأشعّةِ السينيَّةِ أو الماسحاتِ المغناطيسيَّةِ(MRI) ، ووحدةِ الأرشفةِ الصوريَّةِ ، وقاعدةِ بياناتٍ مركزيَّةٍ ، وواجهةِ المستخدمِ للوصولِ إلى الصورِ ، و تُسجَّلُ الصورُ بتنسيقٍ رقميّ وتخزَّنُ في قاعدةِ البياناتِ المركزيَّة .

تتمتَّعُ PACS بعدَّةِ فوائدَ ، و يتيحُ الوصولُ السريعُ والسهلُ إلى الصورِ الطبيَّةِ من مواقع مختلفةٍ ، و يمكنُ للأطبَّاءِ والفرقِ الطبيَّةِ الوصولُ إلى الصورِ من خلالِ نظامِ PACS وتحليلها، مما يؤدّي إلى تشخيصٍ وعلاجٍ فعَّالٍ وتوفيرٍ للوقت ، يمكنُ أيضاً مشاركةُ الصورِ بسهولةٍ مع الفرقِ الطبيَّةِ الأخرى ، ممَّا يسهّلُ التعاونَ والتشاور.

بالإضافةِ إلى ذلك ، يوفّر نظامُ PACS أيضاً سلامةَ وحمايةَ محسّنةً للصورِ الطبيَّة ، من خلالِ التخزينِ الرقميّ ونقلِ الصور، تُقلَّلُ مخاطرُ فقدانِ أو تلفِ الأفلامِ الفيزيائيَّةِ ، و يمكنُ تقييدُ حقوقِ الوصولِ وتطبيقِ تقنيَّاتِ التشفيرِ لضمانِ أن يُوصلَ إلى الصورِ فقط من قبلِ الأشخاصِ المصرَّحِ لهم.

يعدُّ نظامُ PACS جزءاً أساسيَّاً من المرافقِ الطبيَّةِ الحديثةِ و يأخذُ دوراً مهمَّاً في تحسينِ التصويرِ الطبيّ ووضعِ التشخيصِ وتخطيطِ العلاجِ ، و يتيحُ تبادلُ الصورِ الطبيَّةِ بسلاسةٍ وأمانٍ ، ويسهمُ في زيادةِ الكفاءةِ وتحسينِ رعايةِ المرضى .

هي مجموعةٌ من القواعدِ أو التوجيهاتِ الَّتي طُوِّرَتْ لتحقيقِ التوافقِ وتبادلِ البياناتِ بشكلٍ موحّدٍ بينَ مختلفِ الأنظمةِ والمؤسَّسات ، تحدّدُ هذهِ المعاييرُ كيفيَّةَ هيكلةِ وتنسيقِ ونقلِ البياناتِ بهدفِ ضمانِ قدرةِ جميعِ الأطرافِ على تفسيرِ البياناتِ بشكلٍ صحيحٍ واستخدامها بفاعليَّة ، و في مجالِ الرعايةِ الصحيَّة ، هناك معاييرُ متعدّدةٌ لتبادلِ البيانات ، منها :

Health Level Seven (HL7) : هو معيارٌ معترفٌ به دوليَّاً لتبادلِ المعلوماتِ السريريَّةِ والإداريَّةِ في مجالِ الرعايةِ الصحيَّةِ ، و يحدّدُ HL7 تنسيقاتِ البياناتِ وهياكلِ الرسائلِ والبروتوكولاتِ المستخدمةِ في التواصلِ بينَ مختلفِ الأنظمةِ ، مثلَ أنظمةِ معلوماتِ المستشفياتِ وأنظمةِ معلوماتِ المختبراتِ وسجلَّاتِ المرضى الإلكترونية.

Digital Imaging and Communications in Medicine (DICOM):هو معيارٌ لتبادلِ بياناتِ الصورِ الطبيَّةِ ، و يضمنُ DICOM تخزينَ الصورِ الطبيَّةِ بتنسيقٍ موحّدٍ ونقلها بطريقةٍ تضمنُ التفسيرَ الصحيحَ والتحليلَ السليم ، و يتضمَّنُ DICOM ليس فقط بياناتِ الصور نفسها ، ولكنَّهُ يشملُ أيضاً بياناتِ الوصفِ مثلَ معلوماتِ المرضى وتفاصيلِ الفحص.

Consolidated CDA (Clinical Document Architecture) : هو معيارٌ لتبادلِ المستنداتِ السريريَّةِ والتقاريرِ ، مثلَ خطاباتِ الخروجِ وتقاريرِ التشخيصِ ، و يحدّد CDA تمثيلاً مهيكلاً بتنسيقِ XMLيسمحُ بجمعِ المعلوماتِ السريريَّةِ بشكلٍ موحّدٍ وتفسيرها بسهولة .

Fast Healthcare Interoperability Resources (FHIR) : هو معيارٌ حديثٌ لتبادلِ بياناتِ الرعايةِ الصحيَّةِ باستخدامِ واجهاتِ برمجةِ التطبيقات .(APIs) يعتمدُ FHIR على مجموعةٍ من المكوّناتِ البسيطةِ والقابلةِ للتوسعةِ المعروفةِ باسمِ الموارِدِ ، والَّتي تغطّي مختلفَ جوانبِ الرعايةِ الصحيَّةِ يسمحُ FHIR بتبادلِ البياناتِ بينَ الأنظمةِ والتطبيقاتِ المختلفةِ بطريقةٍ فعَّالةٍ ومتوافقة.

تشكّلُ هذه المعايير دوراً مهمَّاً في تعزيزِ تبادلِ البياناتِ في مجالِ الرعايةِ الصحيَّةِ ، وتعزيزِ التوافقِ بينَ الأنظمةِ ، ودعمَ عمليَّاتِ اتّخاذِ القرارِ الطبي ، و تضمنُ أنَّ المعلومات تُتَبادلُ بشكلٍ صحيحٍ وآمنٍ بينَ الأطرافِ المختلفةِ ، ممَّا يؤدّي في النهايةِ إلى تحسينِ رعايةِ المرضى .

Digital Imaging and Communications in Medicine(DICOM)

Digital Imaging and Communications in Medicine (DICOM) :هو تنسيقٌ قياسيٌّ ومواصفةٌ بروتوكوليَّةٌ طُوِّرَتْ خصّيصاً لتخزينِ ونقلِ وعرضِ بياناتِ الصورِ الطبيَّة ، و يتيحُ DICOM تبادلُ الصورِ الطبيَّةِ والمعلوماتِ المرتبطةَ بها بينَ أجهزةٍ وأنظمةٍ طبيَّةٍ مختلفةٍ بغضّ النظرِ عن الشركةِ المصنّعةِ أو المنصَّة .

يضمنُ DICOM تخزينَ ونقلَ الصورِ الطبيَّةِ في تنسيقٍ موحّدٍ بحيثُ يمكنُ قراءتُها وتفسيرُها من قِبلِ أجهزةِ التصويرِ المختلفةِ وبرامجِ عرضِ الصورِ ، و يشملُ هذا القياسيُّ ليس فقط بياناتِ الصورِ نفسها ، ولكنَّهُ يتضمَّنُ أيضاً بياناتِ التوصيفِ مثلَ معلوماتِ المرضى وتفاصيلِ الفحصِ ومعلّماتِ الجهازِوغيرها.

أمَّا استخدامُ DICOM يوفّر عدّةَ فوائد في مجالِ الرعايةِ الصحيَّة :

1ـ التوافق : يتيحُ DICOM تبادلَ الصورِ الطبيَّةِ بسلاسةٍ بينَ أجهزةِ وأنظمةِ تصويرٍ طبيَّةٍ مختلفةٍ بغضّ النظرِ عن الشركةِ المصنّعة أو المنصّة ، و يمكنُ للأطبَّاء والفرقِ الطبيَّةِ عرضُ وتحليلُ ومقارنةُ الصورِ في بيئاتٍ مختلفة .

2ـ ضمانُ الجودةِ : يضمنُ DICOM أنْ تبقى بياناتُ الصورِ غير متغيّرةٍ وذاتَ جودةٍ عاليةٍ طوالَ عمليَّةِ التسجيلِ والنقلِ والعرضِ ،و يضمنُ ذلك تشخيصاً دقيقاً وتخطيطاً فعَّالاً للعلاج .

3ـ الأمانُ والخصوصيَّة : يحتوي DICOM على آلياتٍ لضمانِ سريَّةِ وسلامةِ بياناتِ الصّورِ الطبيَّة. ويتضمَّنُ ذلك حمايةَ المعلوماتِ الصحيَّةِ الشخصيةِ ، ومراقبةَ الوصولِ إلى البياناتِ.

4ـ الأرشفةُ على المدى الطويل : إذ يمكنُ لـ DICOM تخزينُ البياناتِ الطبيَّةِ لفترةٍ طويلةٍ في تنسيقٍ قياسي ، و يتيحُ ذلك إدارةَ البياناتِ واسترجاعها وتحليلها على مدى فترةٍ طويلةٍ من دونِ حدوثِ مشكلاتِ التوافق .

أصبحَ DICOM معياراً صناعيَّاً معترفاً به ويُستخدَمُ على نطاقٍ واسعٍ في المستشفياتِ ، ومراكزِ التصويرِ الطبيّ والمرافقِ الطبيَّةِ الأخرى ، و يشكّلُ دوراً أساسيَّاً في تعزيزِ التوافقِ وتبادلِ الصورِ الطبيَّةِ ويسهم في تحسينِ تشخيصِ الأمراضِ والعلاجِ .

أمثلة توضيحية

الحالة الأولى :

تعرَّضَ مستشفى يملكُ سجلَّاتٍ إلكترونيَّةً شاملةً للمرضى لهجومٍ من قِبلِ قراصنةِ معلومات ، بواسطة استغلالِ ثغرةٍ في نظامِ تكنولوجيا المعلوماتِ الخاصِّ بهم ، و تمكَّنَ المهاجمُ من اختراقِ قاعدةِ البياناتِ وسرقةِ بياناتِ حسَّاسة تخصُّ المرضى ، و تشملُ هذه البياناتُ معلوماتٍ شخصيَّةً مثلَ الأسماءِ وتواريخِ الميلادِ وأرقامِ التأمينِ الاجتماعيّ والتشخيصاتِ الطبيَّة وسجلَّاتِ العلاج.

و تكمنُ أهميَّةُ هذه الحادثةِ في انتهاكِ الخصوصيَّةِ والثقةِ لدى المرضى ، و من خلالِ سرقةِ بياناتِهم الطبيَّةِ الحسَّاسة ، تتعرَّضُ معلوماتُهم الشخصيَّةُ للخطرِ ، وقد تصبحُ في أيدٍ غيرِ مشروعةٍ ، و قد ينتجُ عن ذلكَ سرقةُ الهويَّةِ والأضرارُ الماليَّةُ والأعباءُ العاطفيَّة ، بالإضافة إلى ذلك يمكنُ استخدامُ البياناتِ المسروقةِ لأغراضٍ احتياليَّة ، مثلَ بيعها في السوقِ السوداء ، أو استخدامِها في هجماتِ الصيدِ الاحتيالي .

الحل :

1- هجومُ القراصنةِ على قاعدةِ بياناتِ المستشفى ، وسرقةُ بياناتِ المرضى الحسَّاسةِ يمكنُ أن يشكّلَ انتهاكاً لقانونِ حمايةِ البياناتِ الاتّحادي(BDSG) ، وخاصَّة الفقرة /43/ من BDSG الَّتي تنظّمُ حمايةَ البياناتِ الشخصيَّة .

2- إعطاءُ بياناتِ المرضى للشخصِ الخطأ عن طريقِ الخطأ يمكنُ أيضاً أنْ يشكّلَ انتهاكاً لقانونِ حمايةِ البياناتِ الاتّحادي ، وخاصَّة الفقرة /42/ من BDSG الَّتي تنظّمُ مبدأ الربطِ بالغرضِ في معالجةِ البياناتِ الشخصيَّةِ.

3- الكشفُ غيرِ المصرَّحِ به عن معلوماتٍ طبيَّةٍ لمريض لشخص ثالث غير مخول له بدون موافقة المريض يمكن أن يشكل انتهاكًا للمادة 203 من قانون العقوبات الألماني (StGB) التي تنظم انتهاك سرية المعلومات الطبية.

4- بيعُ بياناتِ المرضى من قِبلِ موظّف في المستشفى لشركاتِ التسويقِ يمكنُ أنْ يشكّلَ انتهاكاً لقانونِ حمايةِ البياناتِ الاتّحادي ، وخاصَّةً الفقرة /44/ من BDSG الَّتي تنظّمُ تجارةَ البياناتِ الشخصيَّة.

5- فقدانُ جهازِ حاسبٍ محمول غير مشفَّرٍ يحتوي على بياناتِ مرضى حسَّاسة من قِبلِ موظَّفٍ في عيادةِ الطبيبِ ، و يمكنُ أنْ يشكّلَ انتهاكاً لمتطلَّباتِ حمايةِ البياناتِ وفقاً للفقرة /9/ من BDSG الَّتي تشترطُ اتّخاذَ التدابيرِ التقنيَّةِ والتنظيميَّةِ المناسبةِ لحمايةِ البيانات .

هذه الفقراتُ القانونيَّةُ ذاتِ الصلةِ تهدفُ إلى ضمانِ حمايةِ بياناتِ المرضى والامتثالِ للقوانينِ فيما يتعلَّقُ بحمايةِ البياناتِ في سياقِ الحالةِ المذكورةِ ، و من المهمّ أنْ تلتزمَ المنشآتُ الطبيَّةُ وموظّفُوها بتلكَ التشريعاتِ لضمانِ خصوصيَّةِ وحمايةِ بياناتِ المرضى.

الحالةُ الثانية :

السيد شميت ، مريضٌ خضعَ لفحصٍ طبيّ شاملٍ في المستشفى مؤخّراً ، و بعدَ انتهاءِ الفحص ، طلبَ نسخةً من النتائجِ الطبيَّةِ لتحويلها إلى أخصائيّ متخصّص ، و للأسف حدثَ خطأ في عمليَّةِ نقلِ البياناتِ ممَّا أدّى إلى الخلطِ في هويَّةِ المستلم.

بدلاً من إرسالِ بياناتِ المرضى إلى الأخصائيّ المطلوب ، أُرسِلَتْ بالخطأ إلى شخصٍ آخر، السيّدة مولر اندهشَتْ السيّدةُ مولر الَّتي ليسَ لديها أيُّ صلةٍ بالسيّد شميت أو علاجِه عندما تلقَّتْ معلوماتِ الصّحةِ الحسَّاسة .

الحل :

الحالةُ المذكورةُ تنطوي على انتهاكٍ لقوانينِ حمايةِ البياناتِ وفقاً للوائحِ العامَّةِ لحمايةِ البياناتِ (DSGVO)وقانون العقوبات.(StGB)

وفقًا للمادة /32/ من DSGVO ، يجبُ حمايةُ البياناتِ الشخصيَّةِ واتّخاذُ التدابيرِ التقنيَّةِ والتنظيميَّةِ الملائمةِ لضمانِ مستوى أمانٍ مناسبٍ ، و في الحالةِ المذكورة ، فشلَتْ المؤسَّسةُ الطبيَّةُ في الوفاءِ بالتزاماتِها بحمايةِ بياناتِ المرضى عن طريقِ تسليمِ المعلوماتِ الحسَّاسةِ بطريقِ الخطأ إلى الشخصِ الخطأ .

و يشكّلُ تسليمُ بياناتِ المرضى إلى أشخاصٍ غيرِ مخوّلينَ انتهاكاً لحقّ الشخصِ في التحكّمِ في معلوماتِه الشخصيَّةِ كما هو موضَّحٌ في المادَّةِ /8/ من DSGVO بالإضافةِ إلى ذلك ، قد يشكّلُ ذلك انتهاكاً للمادَّةِ /203/ من قانونِ العقوباتِ الألمانيّ (StGB) الَّتي تنظّمُ انتهاكَ الأسرارِ الخاصَّة .

وفقاً للمادَّة /203/ من قانونِ العقوبات (StGB) ، يُعدُّ من الجرائمِ إفشاءُ سرٍّ غيرِ مصرَّحٍ بهِ بخاصَّة سرَّاً شخصيَّاً مثلَ الأسرارِ الطبيَّةِ والأدويةِ وأسرارِ المهنِ الطبيَّةِ الأخرى والمحاماةُ والكتبةُ والرعاةُ الروحيّين ومستشاري الضرائبِ ومراقبي الحساباتِ إلخ.

في الحالةِ المذكورة ، قامَتْ المؤسَّسةُ الطبيَّةُ بانتهاكِ هذه الأنظمةِ من خلالِ تسليمِ بياناتِ المرضى إلى شخصٍ غيرِ مخوَّلٍ له الوصولُ إليها ، و قد يكونُ لذلك عواقبُ قانونيَّة ومدنيَّة على المؤسَّسة الطبيَّة.

و من الضروريّ كشفُ وتوثيقُ وإبلاغُ الحالةِ من هذا النوعِ للحفاظِ على حقوقِ خصوصيَّةِ المرضى المتضرّرينَ واتّخاذِ الإجراءاتِ القانونيَّةِ اللّازمةِ ، و يجبُ على المؤسَّسةِ الطبيَّةِ توثيقُ الحادثةِ واتّخاذ تدابيرَ مناسبةٍ لمعالجةِ الانتهاكِ ، وإبلاغِ الجهةِ المختصَّةِ بحمايةِ البياناتِ وفقاً لمتطلبات.DSGVO

الحالة الثالثة :

الدكتورُ أحمد طبيبٌ مؤهَّلٌ بشهادةٍ طبيَّةٍ من دولةٍ خارجِ الاتّحادِ الأوروبيّ ، و يمتلكُ خبرةَ سنواتٍ في طبِّ الأطفالِ ويرغبُ في استخدامِ معرفتِه الطبيَةِ ومهاراتِه في ألمانيا ، ومع ذلك نظراً لعدمِ قبولِ شهادتِه تلقائيَّاً في ألمانيا ، و ليسَ لديهِ حاليَّاً ترخيصٌ لممارسةِ الطب .

و مع ذلكَ ، حرصًا منه على استغلالِ خبرتِه الطبيَّةِ ، يقرّرُ الدكتورُ أحمد العملَ كمستشارٍ طبيٍّ في عيادةِ أطفال ، و في هذا الدور ليس له مسؤوليَّةٌ مباشرةٌ في معالجةِ المرضى ، بل يقدّمُ الدعم للفريقِ الطبيّ في تشخيصِ الحالاتِ ووضعِ خططِ العلاج .

و تشكّلُ حمايةُ البياناتِ دوراً هامَّاً في نشاطِ الدكتور أحمد ، حيثُ يحصلُ على وصولٍ إلى بياناتِ المرضى الحسَّاسة ، و لضمانِ الامتثالِ لحمايةِ البيانات ، و يخضعُ لقواعدَ وتوجيهاتٍ صارمةٍ ، فهو ملزَم بالتعاملِ بسريَّةٍ تامَّةٍ مع جميعِ بياناتِ المرضى والامتثالِ لقوانينِ حمايةِ البياناتِ السارية.

يحصلُ الدكتور أحمد على وصولٍ إلى سجلَّاتِ المرضى الإلكترونيَّة ، الَّتي تحتوي على نتائجِ الفحوصاتِ والتشخيصاتِ الطبيَّةِ وغيرها من المعلوماتِ الحسَّاسةِ ، فهو ملزَم باستخدامِ هذه البياناتِ فقط لأغراضٍ مهنيَّةٍ ، وضمانِ حمايتها من الوصولِ غير المصرَّحِ به.

بالإضافةِ إلى ذلك ، لا يجوزُ للدكتور أحمد الكشفُ عن أيّ معلوماتٍ شخصيَّةٍ أو طبيَّةٍ للمرضى أو مشاركتِها مع أطرافٍ ثالثة ، ما لم يكن هناكَ موافقةٌ صريحةٌ من المريضِ أو وجودِ التزامٍ قانوني بذلك.

تدركُ العيادةُ الَّتي يعملُ فيها الدكتور أحمد أنَّ هذا الحادثَ يمثّلُ انتهاكاً خطيراً لحمايةِ البياناتِ وسريَّةِ بياناتِ المرضى ، تتّخذُ على الفورِ إجراءاتٌ لحذفِ المعلوماتِ الَّتي حُوّلتْ بشكلٍ خاطئٍ ، وضمانِ تجنّبِ وقوعِ أخطاءٍ مماثلةٍ في المستقبل.

الحل :

الدكتور أحمد طبيبٌ مؤهَّلٌ بشكلٍ عالٍ يحملُ درجةً في الطبّ من بلدٍ خارجِ الاتّحادِ الأوروبيّ ، و نظراً لعدمِ اعترافِ درجتِه في ألمانيا ، يقرّرُ العملَ كمستشارٍ طبيّ في عيادةِ أطفال ، و في دوره يحصلُ على وصولٍ إلى سجلَّاتِ المرضى الإلكترونيَّةِ والمعلوماتِ الطبيَّةِ الحسَّاسةِ ، و لضمانِ حمايةِ البياناتِ الشخصيَّةِ ، يخضعُ الدكتور أحمد للقوانينِ والأنظمةِ التالية :

1ـ المادَّةُ 9 من اللائحةِ الأساسيَّةِ لحمايةِ البيانات : و تتناولُ هذه المادَّةُ معالجةَ فئاتٍ خاصَّةٍ من البياناتِ الشخصيَّةِ ، والَّتي تشملُ البياناتِ الصحيَّة ، و تضعُ متطلَّباتٍ صارمةٍ لمعالجةِ مثلِ هذهِ البياناتِ الحسَّاسة.

2ـ المادَّةُ 6 من اللائحةِ الأساسيَّةِ لحمايةِ البياناتِ : تتعاملُ هذه المادَّةُ مع قانونيَّةِ معالجةِ البياناتِ الشخصيَّةِ وتحدّدُ الشروطَ اللازمةَ لمعالجةِ البياناتِ في إطارِ النشاطِ المهني.

3ـ المادَّةُ 32 من اللائحةِ الأساسيَّةِ لحمايةِ البياناتِ: تحدّدُ هذهِ المادَّةُ التدابيرَ المتّخذةَ لحمايةِ البياناتِ الشخصيَّةِ من الفقدانِ ، والاستخدامَ غيرَ المشروعِ أو الوصولِ غيرِ المصرَّح به ، و يلتزمُ مركزُ العيادةِ حيثُ يعملُ الدكتور أحمد بتنفيذِ التدابيرِ التقنيَّةِ والتنظيميَّةِ المناسبةِ لضمانِ أمانِ البيانات.

4ـ المادَّةُ 9 من اللائحةِ الأساسيَّةِ لحمايةِ البياناتِ بالاشتراكِ مع القسمِ 22 من قانونِ حمايةِ البياناتِ الألماني : تسمحُ هذه الأحكامُ بمعالجةِ البياناتِ الصحيَّةِ فقط بشروطٍ محدَّدة ، مثلَ الحصولِ على موافقةٍ

صريحةٍ من المريضِ على أنْ تُعالَجَ بياناتُه من الفريقِ الطبيّ بالشكلِ الَّذي تراهُ الجهةُ المسؤولةُ(العيادةُ في هذه الحالة) ضروريَّاً لإتمامِ العلاج أو للوفاءِ بالتزامٍ قانوني.

بالإضافةِ إلى ذلك، يخضعُ الدكتور أحمد أيضاً لأحكامِ قانونِ العقوبات (StGB) ، وخاصَّةً فيما يتعلَّقُ بحمايةِ الحياةِ الشخصيَّةِ والمجالِ السري وفقاً للمادَّة 203 من قانونِ العقوبات ، يلزِمُه الحفاظَ على سريَّةِ معلوماتِ المرضى وضمانِ سريَّةِ البياناتِ الشخصيَّةِ ، و يعني ذلكَ أنَّه لا يجوزُ له الكشفُ عن أيّ معلوماتٍ شخصيَّةٍ أو طبيَّةٍ من دونِ موافقةٍ صريحةٍ من المريض.

علاوةً على ذلك ، يجبُ على الدكتور أحمد الامتثالُ لقواعدِ المهنةِ الَّتي تحدّدُها غالباً النقاباتُ الطبيَّةُ المعنيَّةُ ، و تشملُ هذه القواعدُ غالباً تعليماتٍ محدَّدةً بشأنِ حمايةِ البياناتِ وسريَّةِ معلوماتِ المرضى.

و تتحمَّلُ العيادةُ الَّتي يعملُ فيها الدكتور أحمد أيضاً مسؤوليَّةَ ضمانِ حمايةِ البياناتِ ، و يجبُ عليها ضمانُ اتّخاذِ التدابيرِ التقنيَّةِ والتنظيميَّةِ المناسبةِ لضمانِ أمانِ بياناتِ المرضى وأنْ يتلقّى جميعُ الموظَّفينَ تدريباً منتظماً حولَ حمايةِ البيانات.

الحالة الرابعة :

تحصلُ إحدى شركاتِ الأدويةِ على وصولٍ إلى قاعدةِ بياناتٍ ضخمةٍ تحتوي على بياناتِ المرضى الَّتي تحصلُ عليها من مؤسَّساتٍ طبيَّةٍ مختلفةٍ ، و تستخدمُ الشركةُ هذه البياناتِ للإعلانِ المستهدفِ لبعضِ الأدويةِ من دونِ الحصولِ على موافقةِ المرضى المعنيّين مسبقاً.

الحل :

تتضمَّنُ بياناتُ المرضى معلوماتٍ حسَّاسةً مثلَ التشخيصاتِ والأدويةِ الموصوفةِ وتاريخَ العلاجِ ، تحلّلُ الشركةُ هذه البياناتِ لتطويرِ حملاتِ تسويقٍ مستهدفةً إرسالَ رسائلَ إعلانيَّةٍ إلى فئاتٍ محدَّدةٍ من المرضى، و نظراً للمعلوماتِ المفصَّلةِ حولَ حالاتِهم الصحيَّةِ، يمكنُ للشركةِ إنشاءُ إعلاناتٍ مخصَّصةٍ تتناسبُ مع احتياجاتِهم ومتطلَّباتِهم الطبيَّةِ الفردية .

استخدامُ هذه البياناتِ الخاصَّةِ بالمرضى لأغراضِ الإعلانِ من دونِ الحصولِ على موافقةِ المرضى يشكّلُ انتهاكاً للخصوصيَّةِ ، ووفقاً للائحةِ العامَّةِ لحمايةِ البيانات (GDPR) ، يُسمَحُ بمعالجةِ البياناتِ الشخصيَّةِ فقط إذا توفّرتْ قاعدةٌ قانونيَّةٌ مثلَ الموافقةِ المُبلِغ عنها مسبقاً أو وجودِ مصلحةٍ مشروعة.

و في هذه الحالة ، لم تحصلْ الشركةُ على موافقةِ المرضى لاستخدامِ بياناتِهم لأغراضِ الإعلانِ، وبالتالي تنتهكُ الشركةُ قوانينَ حمايةِ البياناتِ عن طريقِ معالجةِ البياناتِ الشخصيَّةِ من دونِ أساسٍ قانوني.

المقاطعُ والموادُ ذات الصلة :

-المادّة 6 (قانونيَّة المعالجة) من قواعدِ حمايةِ البياناتِ العامَّة :(GDPR) تحدّدُ هذه المادَّةُ الشروطَ الَّتي يعدُّ فيها معالجةَ البياناتِ الشخصيَّة قانونيَّةً ، بما في ذلك ضرورةَ الحصولِ على موافقةٍ واضحةٍ أو وجودِ مصلحةٍ مشروعة.

-المادَّة 9 (فئاتٌ خاصَّةٌ من البياناتِ الشخصيَّة) من قواعدِ حمايةِ البياناتِ العامَّة :(GDPR) تتناولُ هذه المادّةُ معالجةَ البياناتِ الشخصيَّةِ الحسَّاسة، ومن بينها البياناتُ الصحيَّةُ ، و تضعُ متطلَّباتٍ أكثرَ صرامةً لمعالجةِ هذه البياناتِ ، وتؤكّدُ على حمايةِ الخصوصيَّةِ والمعلوماتِ الحسَّاسة.

-المادة 823 الفقرة 1 من قانونِ الشخصيَّةِ المدنيَّة :(BGB) تنظّمُ هذه الفقرةُ حقَّ الطلبِ تعويضَ المتعرّضين عندَ انتهاكِ حقوقِهم الشخصيَّةِ العامَّةِ، والَّتي تشملُ حمايةَ الخصوصيَّةِ والبياناتِ الشخصيَّة.

-الفقرة 7 من قانونِ مكافحةِ المنافسةِ غيرِ العادلة :(UWG) تحظرُ هذه الفقرةُ أساليبَ الإعلانِ غيرِ النزيهة ، بما في ذلكَ استخدامُ البياناتِ الشخصيَّةِ من دونِ موافقةِ المعنيّين.

الحالة الخامسة :

في أحدِ المستشفياتِ ، يحدثُ حادثٌ تمَّ محو بياناتِ مرضى مهمَّة بطريقِ الخطأ من قبلِ أحدِ الموظَّفينَ، من دونِ توفّرِ نسخٍ احتياطيَّةٍ كافيةٍ ، ويعملُ الموظّفُ على تحديثِ سجلّ المرضى الإلكترونيّ وكانَ يرغبُ في حذفِ ملفٍ غيرِ ضروري ، ولكنْ بدلاً من ذلك ، يختارُ بالخطأ المجلَّدَ الخاطئَ ويحذفُ بياناتِ المرضى المهمَّةِ بشكلٍ لا يمكنُ استعادته.

يترتَّب على هذا الحادثِ آثارٌ خطيرةٌ على عملِ المستشفى ، فبياناتُ المرضى الَّتي حُذِفَت تحتوي على معلوماتٍ عن العلاجاتِ الجاريةِ ، والتشخيصاتِ الطبيَّةِ ، والعمليَّاتِ المخطّطة ، و من دونِ هذه المعلومات، يصعبُ على الأطبَّاءِ والموظَّفينَ الطبيّين تقديمُ الرعايةِ المناسبةِ للمرضى ، وبالتالي تتأثَّرُ جودةُ الرعايةِ الصحيَّةِ .

يكتشفُ المستشفى بسرعةٍ أنَّه لم يجري نسخاً احتياطيَّةً كافيةً لاستعادةِ بياناتِ المرضى المفقودة ، ويصبحُ واضحاً أنَّ فقدان البيانات يمكنُ أن يؤدّي إلى عواقبَ خطيرة ، ليس فقط على المرضى المتأثّرينَ ، ولكن أيضاً على سمعةِ المستشفى وامتثالِه لقوانين حماية البيانات.

الحل

تعرَّضت بياناتُ المرضى الهامَّةُ لحذفٍ غير مقصود من قبلِ أحدِ موظّفي المستشفى من دونِ وجودِ نسخٍ احتياطيَّةٍ كافية ، و يشكّلُ هذا الحادث انتهاكاً لقوانينِ حمايةِ البياناتِ، ولا سيما توجيهاتِ اللائحةِ العامَّةِ لحمايةِ البيانات.(GDPR)

تحدّدُ GDPR أنَّه يجبُ حمايةُ البياناتِ الشخصيَّةُ بشكلٍ مناسبٍ وحمايتها من الفقدانِ أو التدميرِ أو الاستخدامِ غيرِ المصرَّحِ به (المادة 5) ، و وفقاً للمادة /32/ منGDPR ، يُلزَمُ المسؤولون ، مثلُ المستشفى اتّخاذَ تدابير تقنيَّةٍ وتنظيميَّةٍ مناسبةٍ لضمانِ أمان البيانات ، وتشملُ هذه الإجراءاتُ أيضاً إجراءَ نسخٍ احتياطيَّة منتظمةٍ لتجنّبِ فقدانِ البيانات.

يشكّلُ فقدانُ بياناتِ المرضى الهامَّةِ عن طريقِ الخطأ من دونِ وجودِ نسخٍ احتياطيَّةٍ كافيةٍ انتهاكاً لقوانينِ حمايةِ البيانات ، و يُلزَمُ المستشفى بتوثيقِ الحادثِ وإبلاغِ سلطةِ حمايةِ البياناتِ ذاتِ الاختصاصِ إن وجد حسب المادة /33/ و /34/ من (GDPR) و يجبُ إبلاغُ المرضى المتأثّرين بالحادثِ، خاصَّةً إذا كانَ يشكّلُ مخاطرةً كبيرةً على حقوقهم وحرياتهم حسب المادة /34/ من(GDPR) .

و يتعيَّنُ على المستشفى الآن اتّخاذ تدابيرَ مناسبةٍ لمنعِ حدوثِ مثلِ هذه الحوادثِ في المستقبل ، وتشملُ هذه الإجراءاتُ تنفيذَ إجراءاتِ أمانٍ مناسبة ، وتنظيمَ تدريباتٍ منتظمةٍ للموظَّفين بشأنِ حمايةِ البيانات، ومراجعةِ العمليَّاتِ الداخليَّةِ لمعالجةِ البيانات ، و يجبُ على المسؤولينَ ضمانُ اتّخاذِ تدابيرَ تقنيَّةٍ وتنظيميَّةٍ مناسبةٍ لضمانِ سلامةِ وأمانِ بياناتِ المرضى .

حُذِفَتْ البياناتُ الحسَّاسةُ للمرضى عن طريقِ الخطأ من قِبلِ أحدِ موظّفي المستشفى من دونِ وجودِ نسخٍ احتياطيَّةٍ كافيةٍ ، و يمكنُ أن يكونَ لهذا الحادثِ عواقبُ جنائيَّةٌ وفقاً للمادة /a303/ من قانون العقوبات (تزييف البيانات) والمادَّة /263/ من قانونِ العقوبات (الاحتيال).

وفقًا للمادة /a303/ من قانون العقوبات، يُعاقبُ أيُّ شخصٍ يقومُ بتزييفِ أو حذفِ أو إخفاءِ البياناتِ غيرِ المصرَّحِ بها والَّتي تُخزَّنُ من دونِ إذنٍ من المخوَّلِ لهم ، و بما أنَّ الموظَّفَ حذفَ البياناتِ عن طريق الخطأ ولم يتم إجراءُ نسخٍ احتياطيَّةٍ كافية ، يمكن وصفُ ذلك تزويراً للبيانات .

بالإضافةِ إلى ذلك ، يمكنُ وصفُ الحادثِ أيضاً احتيالاً ، ووفقاً للمادَّةِ /263/ من قانونِ العقوبات ،و من خلالِ حذفِ البياناتِ الحسَّاسة للمرضى عن طريق الخطأ، يمكنُ أن يكونَ لدى الموظَّف النيةُ للتسببِ بضررٍ في الممتلكات ، و في هذه الحالةِ سيكونُ الضررُ هو فقدانُ بياناتِ المرضى ، مما يؤدّي إلى تأثيراتٍ على رعايةِ المرضى وربَّما تبعاتٍ قانونيَّة أو مالية .

الحالة السادسة :

تُجري شركة بحوثٍ طبيَّة دراسةً حولَ فعاليةِ دواءٍ جديدٍ تمَّ تطويره ، وللحصولِ على نتائجَ موثوقةٍ ، تحتاجُ الشركةُ الوصولَ إلى بياناتِ المرضى الَّتي تحتوي على معلوماتٍ حولَ تطوّرِ المرضِ والعلاجِ وحالة الصحة .

تقرّرُ الشركةُ استخدامَ بياناتِ المرضى من مختلفِ المؤسَّساتِ الطبيَّةِ من دونِ الحصولِ على الموافقة المطلوبةِ من المرضى المعنيّين ، و تتجاهلُ الشركةُ الترتيباتِ القانونيَّة المتعلّقةَ بحمايةِ البياناتِ الشخصيَّةِ وتصريحِ الموافقة .

عندما يصلُ الجمهورُ إلى علمٍ بمثلِ هذه الممارسات، ينشأ جدلٌ كبيرٌ ، و يوجّه المرضى ونشطاءُ حقوق الخصوصيَّةِ اتّهامات بانتهاكِ الخصوصيَّة وعدمِ الحصولِ على موافقةٍ مطلوبة ، و تواجهُ الشركةُ ضغوطاً لتبريرِ إجراءاتها واتّخاذ إجراءاتٍ لحمايةِ خصوصيَّةِ المرضى المعنيين.

الحل :

تتناولُ هذه الحالة وجودَ شركةٍ للبحوثِ الطبيَّةِ تستخدمُ بياناتِ المرضى لأغراضِ الدراسات ، من دونِ الحصولِ على الموافقةِ المطلوبةِ من المرضى المعنيين ، و هذا الإجراء يشكّلُ انتهاكاً لقوانينِ حمايةِ البياناتِ السارية ، وفيما يلي الفقراتُ القانونيَّةُ المعنية :

1ـ متطلَّباتُ الموافقة : وفقاً للمادَّة /6/ الفقرة (a1) من اللائحةِ العامَّةِ لحمايةِ البيانات (GDPR) ، تكونُ معالجةُ البياناتِ الشخصيَّةِ قانونيَّة فقط إذا قدَّمَ الشخصُ المعنيُّ موافقته على ذلك ، و في هذه الحالة تنقصُ الموافقةُ من المرضى ، ممَّا يعني أنَّ معالجةَ البياناتِ غير قانونية.

2ـ التزاماتُ الإفصاح : وفقاً للمادَّةِ /13/ والمادَّة /14/ من قانونِ حمايةِ البياناتِ العام(GDPR) ، يجبُ على الشركاتِ إبلاغُ الأشخاصِ المعنيّين بمعالجةِ بياناتِهم الشخصيَّة ، بما في ذلكَ الغرضَ من المعالجة، والأساسَ القانوني، وفي بعضِ الحالاتِ تُعطى المعلوماتُ لأطرافٍ ثالثة ، و في هذه الحالة لم يُبلَغ المرضى المعنيّون بشكلٍ سليمٍ بشأنِ استخدامِ بياناتِهم لأغراضِ الدراسات.

3ـ استثناءاتُ البحوث : على الرغمِ من أنَّ البحوث تمثّلُ غرضاً شرعيَّاً، إلا أنَّ هناك أحكاماً خاصَّةً لمعالجةِ البياناتِ الشخصيَّةِ لأغراضِ البحثِ ، و وفقاً للمادة /27/ من قانونِ حمايةِ البياناتِ الاتّحادي (BDSG)، يجبُ على مشروعاتِ البحثِ أنْ تلبّي بعضَ المتطلَّبات ، بما في ذلكَ معالجةَ البياناتِ المناسبةِ وحفظَ حقوقِ وحريَّاتِ الأشخاصِ المعنيين.

و في هذه الحالة ، انتهكَتْ الشركةُ أحكامَ حمايةِ البياناتِ من خلالِ استخدامِ بياناتِ المرضى من دونِ الحصولِ على الموافقةِ اللازمةِ لأغراضِ البحث ، و يمكنُ أنْ يكونَ لهذا الإجراءِ عواقب قانونية ، بما في ذلك فرضُ غراماتٍ ماليَّةٍ وفقاً للمادَّة /83/ من قانونِ حمايةِ البياناتِ العامَّة (GDPR) ومطالبات مدنيَّة للمرضى المتضرّرين بالتعويضِ وفقاً للمادَّة /82/ من قانونِ حمايةِ البياناتِ العامَّة(GDPR) .

الحالةُ السابعة :

يقومُ أحدُ موظَّفي مقدّمي الرعايةِ الصحيَّةِ بالخطأ بنشرِ تقريرٍ يحتوي على بياناتٍ حسّاسةٍ للمرضى على

موقعٍ عام على الانترنت ، و يتضمَّنُ التقريرُ معلوماتٍ سريَّةٍ مثلَ التشخيصاتِ وتاريخِ العلاجِ ومعلوماتِ التعريفِ الشخصيَّة للمرضى ، اختِيرَ الموظَّفُ بالخطأ خياراً غيرَ صحيحٍ عندَ تحميلِ التقريرِ، ولاحظ خطأه فقط في وقت لاحق.

الحل :

يُفصحُ أحدُ موظَّفي تقديمِ خدماتِ الرعايةِ الصحيَّةِ عن طريقِ الخطأ عن تقريرٍ يحتوي على بياناتٍ حسَّاسةٍ للمرضى على موقعٍ ويب عام ، ويعدُّ هذا انتهاكاً لخصوصيَّةِ وسريَّةِ بياناتِ المرضى .

الموادُ القانونيَّةُ ذات الصلة :

1- المادَّة /9/ من لائحةِ حمايةِ البياناتِ العامَّة :(GDPR) تنظّم هذه المادَّةُ حمايةَ البياناتِ الصحيَّةِ الشخصيَّةِ ، وتضمنُ حمايةَ المعلوماتِ الحسَّاسة بطريقةٍ مناسبة .

2- المادّة /203/ من قانونِ العقوباتِ الألماني : تتناولُ هذه المادّةُ انتهاكَ الأسرارِ الخاصَّةِ بالأفراد ، بما في ذلك الكشفُ عن بياناتِ مرضى سريَّةٍ من دونِ موافقة .

3- المادَّةُ /43/ من قانونِ حمايةِ البياناتِ الاتّحادي الألماني : تحتوي هذه المادَّةُ على أحكامٍ تتعلَّقُ بمعالجةِ البياناتِ الشخصيَّةِ في قطاعِ الرعايةِ الصحيَّةِ ، وتنصُّ على ضرورةِ حمايةِ بياناتِ الصّحةِ الحسَّاسةِ بشكلٍ خاص .

إنَّ نشرَ بياناتِ حسَّاسةٍ للمرضى على موقعٍ ويب عام يتعارضُ مع هذه القوانينِ ، ويمكنُ أنْ يكونَ له عواقبُ جنائيَّةٌ ومدنيَّةٌ على الموظَّف ومقدّمِ الخدمةِ الصحيَّةِ ، و من المهمّ تنفيذُ التدابيرِ التقنيَّةِ والتنظيميّةِ المناسبةِ لضمانِ سريَّةِ وأمانِ بياناتِ المرضى وتجنّبِ انتهاكاتِ حمايةِ البيانات ، يشملُ ذلك إجراءاتِ أمانٍ مثلَ ضوابطِ الوصولِ والتشفيرِ وتدريبِ الموظّفينَ بشكلٍ منتظَم والامتثالِ للتشريعاتِ النافذةِ لحمايةِ البيانات .

الحالة الثامنة :

يُدعى المريضُ ماكس مولر وقد تلقى حديثاً العلاجَ الطبيَّ في مستشفى ، و بعدَ بضعةِ أسابيع ، يلاحِظُ أنَّهُ يتلقَّى فواتيرَ طبيَّةً غيرَ معتادةٍ ولا يستطيعُ توجيهها ، بالإضافةِ إلى ذلك يتلقى مطالباتٍ تأمينيَّةً لخدماتٍ طبيَّةٍ لم يتلقها أبداً .

و يشعرُ ماكس مولر بالشكّ ويتّصلُ بالمستشفى وشركةِ التأمينِ الخاصَّةِ به لتوضيحِ الأمر، فيتبيَّنُ أنَّ هناكَ تسرّبٌ للبياناتِ ، حيثُ سُرِقت المعلوماتُ الشخصيَّة والطبيَّةُ لماكس مولر ، و استخدمَ شخصٌ مجهولٌ هذه المعلوماتِ لتقديمِ فواتيرَ طبيَّة ومطالباتٍ تأمينيَّةٍ بالنيابةِ عن ماكس مولر.

و تكمنُ أهميَّةُ هذه الحالةِ في أنَّه من خلالِ تسرّبِ البياناتِ وسرقةِ الهويّة ، تسقطُ معلوماتُ ماكس مولر الشخصيَّةُ والطبيَّةُ في أيدٍ خاطئة.

الحل :

في الحالةِ المذكورةِ أعلاه ، حيثُ يتلقّى المريضُ فواتير طبيَّة غيرَ مصرَّحٍ بها ، ومطالباتٍ للحصولِ على خدماتٍ طبيَّةٍ غيرِ مقدَّمةٍ بسببِ تسرّبِ البياناتِ وسرقةِ الهويَّة ، يمكنُ أن تكونَ هناكَ عدّةُ موادٍ قانونيَّةٍ ذاتِ صلةٍ لضمانِ حمايةِ البياناتِ الشخصيَّةِ وحقوقِ المريض ، ومن بينِ هذه الموادِ القانونيَّةِ المُحتملة :

1ـ المادَّةُ /7/ الفقرةُ /1/ من قانونِ حمايةِ البياناتِ الاتّحادي :(BDSG) تحدّدُ هذه المادَّةُ المبادئَ العامَّةَ لحمايةِ البياناتِ ، بما في ذلكَ التزامَ حمايةِ البياناتِ الشخصيَّةِ ومنعَ الوصولِ غيرِ المصرَّحِ به وسوءَ الاستخدام .

2ـ المادَّةُ /43/ من قانونِ حمايةِ البياناتِ الاتّحادي :(BDSG) تنظمُ هذه المادَّةُ التزامَ الإبلاغِ عن انتهاكاتِ حمايةِ البيانات في حالةِ تسرّبِ البياناتِ الَّذي يؤدّي إلى سرقةِ الهويَّة ، قد يكونُ من المطلوبِ على المؤسَّسةِ الطبيَّةِ المتضرّرةِ الإبلاغَ عن ذلك للهيئاتِ الإشرافيَّةِ المعنيَّة.

3ـ المادَّةُ /823/ الفقرة /1/ من قانونِ الشركاتِ المدنيَّةِ :(BGB) تنظّمُ هذه المادَّةُ حقوقَ التعويضِ في حالةِ السلوكِ غيرِ القانوني ، و يمكنُ للمريضِ أنْ يقدّمَ مطالبةَ تعويضٍ بسببِ الفواتيرِ الطبيَّةِ غيرِ المصرَّحِ بها ومطالباتِ الخدماتِ الَّتي لم يتلقّها.

4ـ المادَّةُ /203/ من قانونِ العقوباتِ :(StGB) تنظّمُ هذه المادَّةُ سريَّةَ المهنةِ وحمايةَ البياناتِ الشخصيَّةِ من قبلِ فئاتٍ معيَّنةٍ من المهنِ مثلَ الأطبَّاء ، و في حالةِ الوصولِ غيرِ المصرَّحِ به أو الكشفِ عن بياناتِ المرضى، يمكنُ اتّخاذُ إجراءاتٍ قانونية .

هذه الموادُ القانونيَّةُ هي أمثلةٌ ويمكنُ أنْ تختلفَ حسبَ الحالةِ المحدّدةِ والقوانين النافذة ، و من المهمّ مراعاةُ الأنظمةِ القانونيَّةِ والتشريعاتِ المعمولِ بها لضمانِ حمايةِ البياناتِ الشخصيَّةِ في الرعايةِ الصحيَّةِ والتعاملِ بشكلٍ مناسبٍ مع أيّ انتهاكاتٍ قانونيَّةٍ محتملة .

الحالةُ التاسعة :

السيدة مولر تتلقَّى العلاجَ منذُ بضعةِ أشهرٍ بسببِ مرضٍ مزمنٍ ، و في أثناءِ استشارةٍ طبيَّةٍ ، يشاركُ الطبيب المعالج الدكتور شميت معلوماتٍ طبيَّةً مع زوجِها السيد مولر، من دونِ الحصولِ على موافقةٍ صريحةٍ من السيّدة مولر ، تتضمَّنُ هذه المعلوماتُ التشخيصاتُ وتطوّراتُ العلاجِ ومعلوماتٍ صحيَّةٍ حسَّاسة أخرى .

الحل :

في الحالةِ المذكورةِ ، يتعلّقُ الأمرُ بانتهاكِ للخصوصيَّةِ ولسريَّةِ المعلوماتِ الطبيَّة بموجبِ المادَّة /203/ من قانونِ العقوباتِ الألماني (StGB) بالاشتراكِ مع المادَّةِ MBO-Ä9 ، بموجبِ هذه الأحكامِ ، يتوجَّبُ على الطبيبِ الالتزامُ بسريَّةِ المعلوماتِ الطبيَّةِ ومعاملتَها بسريَّة ، وبالتالي يُعدُّ تبادلُ المعلوماتِ الطبيَّةِ مع أحدِ أفرادِ العائلةِ من دونِ الحصولِ على موافقةٍ صريحةٍ من المريضِ انتهاكاً لهذهِ الواجبات.

علاوةً على ذلك ، تُنظَّمُ حمايةُ البياناتِ في قطَّاعِ الرعايةِ الصحيَّةِ من خلالِ قانونِ حمايةِ البياناتِ الألماني (BDSG)، ولائحةِ الحمايةِ الأوروبيَّةِ العامَّة للبيانات .(GDPR) و تضمنُ هذه القوانينُ أنْ تُحمى البياناتُ الشخصيَّةُ ، بما في ذلكَ المعلوماتِ الطبيَّة ، بشكلٍ مناسبٍ وأنَّهُ يجوزُ تبادلها فقط بالموافقةِ أو بموجبِ أساسٍ قانوني.

و في الحالة المعيَّنة ، كانَ يتعيَّنُ على الطبيبِ المعالجِ أنْ يحصلَ على موافقةٍ صريحةٍ من المريضةِ قبل تبادلِ المعلوماتِ الطبيَّةِ مع زوجها ، و هذا الإجراءُ يتوافقُ مع مبدأ الموافقةِ الصريحةِ بموجبِ المادَّة/6/ من قانونِ حمايةِ البياناتِ العامَّة (GDPR) والمادة /630/ dالفقرة 1 من قانونِ الشفاء .

إنَّ الموافقةَ الصريحة هي شرطٌ أساسيٌّ لمعالجةِ البياناتِ الشخصيَّة بشكلٍ قانوني ، بما في ذلكَ المعلوماتِ الطبيَّة .

و عدمُ الامتثالِ لهذه الأحكامِ القانونيَّةِ يمكنُ أنْ يؤدّي إلى عواقبَ قانونيَّة ، بما في ذلكَ فرضُ غراماتٍ ماليَّةٍ وفقاً للمادَّة /83/ من قانونِ حمايةِ البياناتِ العامَّة (GDPR) أو ملاحقةٍ قضائيَّةٍ بموجبِ المادَّة/203/ من قانونِ العقوباتِ الألماني .(StGB) علاوةً على ذلك ، قد تنشأ مطالباتٌ قضائيَّةٌ مدنيَّةٌ

بتعويضٍ مادّي وتعويضٍ للأضرارِ المعنويَّةِ من جانبِ المريض إذا تسبَّب له تبادل المعلوماتِ الطبيَّة غير المصرَّح بها في وقوعِ أضرارٍ له .

الحالة العاشرة :

يقومُ معهدُ بحوثٍ طبيَّةٍ بإجراءِ دراسةٍ حولَ فعاليَّةِ طريقةِ علاجٍ جديدة ، تُجمَعُ بياناتُ المرضى المجهولة الهويَّةِ من مستشفياتٍ مختلفةٍ للدراسة ، ويشاركُ المعهدُ البياناتِ مع شركاءٍ خارجيّينَ لإجراءِ تحليلٍ شامل ومع ذلكَ يتّضحُ أنَّ عمليَّةَ إلغاءِ التعريفِ للبياناتِ لم تكنْ كافيةً ، وأنَّ معلوماتٍ محدَّدةً مثلَ العمرِ والجنسِ والتشخيصِ الطبيّ يمكنُ تتبّعها بسهولةٍ بواسطةٍ مصادرِ بياناتٍ أخرى متاحة ، و بالتالي يمكنُ تتبّعُ البياناتِ الَّتي أُلغيَ تعريفُها في الأصل ، ويكونُ هناكَ خطرُ تعريضِ خصوصيَّةِ المرضى للخطر.
والمرضى المعنيّونَ قلقونَ من أنْ يُكشّفَ عن معلوماتِهم الشخصيَّة ، ممَّا يمكنُ أنْ يؤدّي إلى سرقةِ الهويةِ أو التمييز ، و يتعيَّنُ على المعهدِ البحثي أنْ يتّخذَ على وجهِ السرعةِ إجراءاتٍ لضمانِ إلغاءِ التعريفِ المناسبِ للبياناتِ ، وحماية خصوصيَّةِ المرضى ، ويتطلَّبُ ذلك مراجعةَ عمليَّاتِ مشاركةِ البياناتِ والتعاونَ الوثيقَ مع الشركاءِ الخارجيّين لضمانِ الامتثالِ لجميعِ معاييرِ حمايةِ البياناتِ الضروريَّة.

الحل :

الحالةُ المذكورةُ تصفُ وضعيَّةَ حيث يشاركُ معهد بحثٍ طبي بياناتِ المرضى المجهولةِ الهويَّةِ مع أطرافٍ ثالثة ، لكنْ يمكنُ تتبّعها بسهولةٍ ، وتهدّدُ خصوصيَّةَ المرضى في هذه الحالة ، و تكون الموادُ القانونيَّةُ التاليةُ ذات الصلة :

1ـ اللائحةُ العامَّةُ لحمايةِ البيانات :(GDPR) تضع GDPR قواعدَ صارمةً للتعاملِ مع البياناتِ الشخصيَّةِ وتلزمُ المنظَّماتِ باتّخاذِ تدابيرَ تقنيَّة وتنظيميَّة مناسبةً لضمانِ أمانِ وسريَّة البيانات .

2ـ قانونُ حمايةِ البياناتِ الألماني :(BDSG) يحتوي BDSG على أحكامٍ تتعلَّقُ بمعالجةِ البياناتِ الشخصيَّةِ في ألمانيا بشكلٍ خاص ، و إنَّ القسمَ المتعلّقَ بمعالجةِ البياناتِ لأغراضٍ علميَّة (§§ 22-26 BDSG) ذات صلة بنقلِ واستخدامِ بياناتِ المرضى في المعاهدِ البحثيَّة الطبيَّة .

3ـ قانونُ الأجهزةِ الطبيَّةِ :(MPG) يحتوي MPG على قواعدَ لاستخدامِ الأجهزةِ والمنتجاتِ الطبيَّةِ ، و عندَ معالجةِ بياناتِ المرضى في سياقِ البحثِ وتطويرِ المنتجاتِ الطبيَّة ، يجبُ الامتثال لأحكام MPG

4ـ القانونُ الجنائيُّ : (StGB) يحتوي StGB على أحكامٍ تتعلَّق بالجرائمِ ، بما في ذلكَ حمايةُ سريَّةِ بياناتِ المرضى بشكلٍ خاص ، و قد يكونُ القسم /203/ من القانونِ الجنائيّ ذا صلةٍ في هذهِ الحالةِ ، الَّذي ينظّمُ انتهاكَ سريَّةِ الأطبَّاءِ أو المعالجين النفسيّين .

و من المهمّ أن يلتزمَ المعهدُ البحثيُّ الطبيُّ بالقوانينِ واللوائحِ المناسبةِ لضمانِ خصوصيَّةِ وحمايةِ بياناتِ المرضى المعنيّين ، و يعدُّ الامتثالُ لهذهِ القوانينِ ضروريَّاً للحفاظِ على ثقةِ المرضى في التعاملِ مع بياناتِهم الصحيَّةِ الحسَّاسةِ وتجنّبِ أيّ عواقب قانونيَّة محتملة .

الحالة الحادية عشر :

تنقلُ شركةٌ تقدّمُ خدماتٍ طبيَّةً عن بعد بتسجيلاتِ فيديو غيرِ مشفَّرةٍ للمرضى إلى خوادم غيرِ آمنة ، ممَّا يؤدّي إلى انتهاكٍ للخصوصية .

و نتيجةً لهذا النقلِ غيرِ الآمن ، يمكنُ لمهاجمٍ خارجيّ الوصولُ إلى تسجيلاتِ الفيديو وربّما الحصول على معلوماتٍ صحيَّةٍ حسَّاسةٍ للمرضى ، وهذا يشكّلُ انتهاكاً خطيراً للخصوصيَّةِ ، حيثُ يتعرَّضُ سريَّة وسلامة بيانات المرضى للخطر .

الحل :

تصفُ الحالةُ المذكورةُ وضعيَّةً ، حيث تنقلُ شركةُ تقديمِ خدماتٍ الطبّ عن بُعد تسجيلاتِ فيديو غيرِ مشفَّرةٍ للمرضى إلى خوادم غيرِ آمنةٍ ، ممَّا يؤدّي إلى انتهاكٍ للخصوصيَّةِ ، و في هذه الحالة، تكون الأحكامُ القانونيَّةُ التاليةُ ذاتِ الصلة :

1ـ اللائحةُ العامَّةُ لحمايةِ البياناتِ :(GDPR) تضعُ GDPR قواعدَ صارمةً لحمايةِ البياناتِ الشخصيَّةِ، بما في ذلك الأمان في عمليَّةِ النقلِ والتخزين ، و المادَّةُ /32/ من GDPR تلزَمُ الشركاتُ باتّخاذِ تدابير تقنيَّة وتنظيميَّة مناسبةٍ لضمانِ أمانِ المعالجة .

2ـ قانونُ الاتّصالاتِ الإلكترونية :(TMG) ينظّمُ قانونُ الاتّصالات الإلكترونيَّة حمايةَ البياناتِ في مجالِ الطب عن بُعد ، ويضعُ الالتزاماتِ على مقدّمي خدماتِ الطب عن بُعد بشكلٍ خاص، و تنظّمُ المادّة /13/ من TMG أمانَ عمليَّة نقلِ البياناتِ وتتطلَّبُ اتّخاذَ تدابير حمايةٍ مناسبة .

3ـ قانونُ حمايةِ البيانات الألماني :(BDSG) يحتوي BDSG على أحكامٍ لحمايةِ البياناتِ الشخصيَّةِ في ألمانيا بشكل خاص ، و تنظّمُ المادَّة /9/ من BDSG التدابيرَ التقنيَّة والتنظيميَّة الَّتي يجبُ على الشركاتِ اتّخاذُها لضمانِ سريَّةِ وسلامةِ وتوفّرِ البيانات .

و يمكن أن يؤدّي عدمُ الامتثالِ لهذه القوانين والتشريعات إلى عواقبَ قانونيَّةٍ خطيرة ، بما في ذلكَ فرض غراماتٍ ماليَّةٍ ومطالباتٍ بالتعويض ، و يجبُ على الشركاتِ الَّتي تقدّمُ خدماتِ الطبّ عن بُعد ضمانَ أنَّها تتّخذُ التدابيرَ التقنيَّة والتنظيميَّة اللَّازمةَ لضمانِ سلامةِ البياناتِ المنقولة وتجنّب انتهاكاتِ حماية البيانات.

الحالة الثانية عشر :

يستخدمُ الطبيبُ منصَّةَ ذكاءٍ اصطناعي تسمىChatGPT لإنشاءِ توثيقٍ لحالاتِ المرضى .

و في حالةٍ معيَنة ، يدخلُ الطبيبُ بياناتٍ طبيَّة لمريضٍ في محادثةٍ مع الروبوت لتوثيقِ المعلوماتِ ذاتِ الصلةِ لملفِ الحالة ، و يعالجُ الروبوت البياناتِ وإنشاءَ توثيقٍ تفصيلي للحالةِ تلقائيَّاً.

الحل :

في الحالةِ المذكورة ، يتبادلُ الطبيبُ بياناتٍ طبيَّةً لمريضٍ مع برنامجِ الدردشةِ لإنشاءِ توثيقٍ لحالته ، و في هذا السياقِ ، تكونُ المادَّةُ القانونيَّةُ ذات الصلةِ كالتالي :

1ـ اللائحةُ العامَّة لحمايةِ البيانات :(GDPR) تنظّم GDPR حمايةَ البياناتِ الشخصيَّة ، وتحدّدُ قواعد معالجةِ البياناتِ ونقلها ، و المادة /6/ من GDPR تحدّد قانونيَّةَ معالجةَ البيانات ، بينما المادَّة /9/ تتعامل مع فئاتٍ خاصّة من البيانات ، بما في ذلكَ البيانات الصحية.

2ـ قانون حماية البيانات الألماني :(BDSG) ينفذ قانون حماية البيانات الألماني GDPR في القانون المحلي ، و المادَّةُ /22/ من BDSG تنظّمُ معالجةَ البياناتِ الصحيَّة، بينما المادَّة /26/ تسمحُ بمعالجةِ البياناتِ الشخصيَّةِ لأغراضِ الرعايةِ الصحيَّة .

3ـ الأنظمةُ المهنيَّةُ : يخضعُ الأطبَّاءُ لالتزاماتٍ مهنيَّة تنظّمُ سريَّةَ المعلوماتِ الطبية ، على سبيلِ المثال، يشملُ ذلك السرَّ المهنيَّ للأطبَّاءِ بموجبِ المادّة /9/ من تعليماتِ المهنة الطبية .

4ـ المادَّة /203/ من القانونِ الجنائي (انتهاك السر المهني): تنظّمُ هذه المادَّةُ حمايةَ الأسرارِ الشخصيَّةِ، بما في ذلكَ البياناتِ الطبيَّة ، و يمكنُ أن يكونَ تحويلُ البياناتِ الطبيَّةِ من دونِ موافقةِ المريضِ انتهاكاً للسرّ المهني .

5ـ المادَّة /203أ / من القانونِ الجنائي (انتهاك سرية المعلومات الضريبية): تتعلَّقُ هذه المادَّةُ بسريَّةِ المعلومات الضريبية ، و في السياق الطبي، قد تكونُ بعضُ المعلوماتِ الضريبيَّةُ ذاتِ الصلةِ بعلاجِ المريضِ ذاتَ أهميَّةٍ ، ويمكنُ أن يكونَ نقلُ هذه البياناتِ من دونِ إذنٍ انتهاكاً لسريَّةِ المعلوماتِ الضريبية.

6ـ المادَّة /203ب/ من القانونِ الجنائي (انتهاك السرية المهنية): تتعلَّقُ هذه المادَّةُ بحمايةِ الأسرارِ المهنيَّة، بما في ذلكَ المعلوماتِ الطبيَّةَ الَّتي يتعرَّفُ عليها الأطبَّاءُ في أثناءِ مزاولةِ مهنتِهم ، و يمكنُ أنْ يكونَ نقلُ مثل هذه المعلوماتِ من دونِ وجودِ مصلحةٍ مشروعةٍ أو موافقةٍ انتهاكاً للسريَّةِ المهنيَّةِ .

و يمكن أن يترتَّبَ على الامتثال لهذه المواد القانونيَّة عواقب قانونيَّة جنائيَّة ، مثلَ الغراماتِ الماليَّةِ أو السجن ، لذا يلتزمُ الأطبَّاءُ بالحفاظِ على سريَّةِ البياناتِ الطبيَّةِ وتحويلِها فقط وفقاً للقوانين .

يتوجَّبُ الامتثالُ لهذه القوانينِ واللوائح لضمانِ حمايةِ خصوصيَّةِ وبياناتِ المرضى الطبيَّةِ الحسَّاسة ، و يجبُ على الطبيبِ التأكُّدُ من أنَّ نقلَ البياناتِ إلى برنامجِ الدردشةِ ومعالجتِها يتم وفقاً للقوانينِ والتشريعاتِ المعمولِ بها ، ويشملُ ذلك الحصولَ على موافقةِ المريض ، وتوفيرَ التدابيرِ التقنيَّةِ والتنظيميَّةِ المناسبةِ لحمايةِ البيانات ، واحترامَ مبدأ الاقتصارِ على البياناتِ المطلوبةِ ومبدأ التحصينِ بالغرض .

الحالة الثالثة عشر :

يعتمد طفل قاصر فحوصات وعلاجات طبية. بعد الانتهاء من الفحوصات، من المفترض أن تُعرض النتائج على والدي الطفل، كما هو الحال عادةً. ومع ذلك، يعبر الطفل عن رغبته في عدم إظهار النتائج لوالديه، خشية من تداعيات سلبية أو انتهاك لخصوصيته.

تكمن أهمية هذه الحالة في احترام حق التصرف بالمعلومات الشخصية والخصوصية، وخاصةً بالنسبة للأطفال القاصرين ، و رغبة الطفل في عدم إعلام والديه بمعلوماته الطبية تشكل تحديًا، حيث يتم عادةً احترام حق الآباء في معرفة معلومات صحة أطفالهم.

الحل :

في الحالة المذكورة، يعبر طفل قاصر عن رغبته في عدم مشاركة نتائج الفحوصات الطبية مع والديه.

1ـ المادة /630د/ من قانون العقوبات المدني (موافقة المريض): تنظم هذه المادة حق المريض في الموافقة على العلاج الطبي ومعالجة بياناته. عادةً ما يكون لدى الأطفال قاصرين حق المشاركة ويتطلب موافقتهم، إذا كان لديهم القدرة اللازمة للتمييز.

2ـ المادة /630ف/ من قانون العقوبات المدني (توثيق العلاج): تحدد هذه المادة متطلبات توثيق العلاج الطبي. من المهم أن يتم توثيق السجلات الطبية بشكل صحيح وكامل لضمان الرعاية الصحية المناسبة.

3ـ المادة /203/ من قانون العقوبات المدني (انتهاك السر المهني): تنظم هذه المادة حماية الأسرار الشخصية، بما في ذلك المعلومات الطبية. يمكن أن يكون تحويل المعلومات الطبية بدون موافقة انتهاكًا للسر المهني.

4ـ قانون حقوق المرضى(PatientenRG): يعزز هذا القانون حقوق المرضى ويؤكد على استقلالية المعلومات الشخصية والخصوصية. يتضمن أحكامًا لحماية بيانات الأطفال القاصرين وضمان حقوقهم في معالجة المعلومات الطبية.

عند النظر في عمر الطفل، يجب على الأطباء والموظفين الطبيين احترام رغبة الطفل، إذا كان لديه القدرة اللازمة للتمييز. يجب أن يعثروا على حلول بديلة لحماية خصوصية الطفل وفي نفس الوقت ضمان تلقيه الرعاية الطبية المناسبة. يمكن أن تشمل هذه الحلول إجراء محادثات سرية، واستشارة أخصائي علاج الأطفال والمراهقين، واعتبار التقدير الذاتي للطفل.

الحالة الرابعة عشر :

يطرحُ أحدُ الأطبَّاءِ أسئلةً على أحد أفرادِ أسرةِ مريضٍ للحصول على معلومات طبية حول حالته الصحية، دون الحصول على موافقة صريحة من المريض.

تكمن أهمية هذه الحالة في حماية الخصوصية وحق التحكم في المعلومات الشخصية للمريض. يحق لكل مريض أن يتحكم في كشف واستخدام معلوماته الطبية.

الحل :

في الحالة المذكورة، يقوم الطبيب بسؤال أحد أفراد عائلة المريض عن معلومات طبية دون الحصول على موافقة صريحة من المريض. في هذا السياق، المواد القانونية ذات الصلة هي كالتالي:

1- المادة 9 (2) (h) من قانون حماية البيانات العامة :(DSGVO) تنص هذه المادة على أن معالجة الفئات الخاصة من البيانات الشخصية، بما في ذلك البيانات الصحية، غير مسموح بها إلا بناءً على موافقة صريحة من الشخص المعني.

2- المادة /203/ من قانون العقوبات المدني (انتهاك الأسرار الشخصية): تحمي هذه المادة حق الأسرار الشخصية وتحظر الكشف غير المصرح به للمعلومات، بما في ذلك البيانات الطبية، دون موافقة الشخص المعني.

في الحالة المذكورة، ناقشَ الطبيبُ المعلوماتِ الطبية مع أحد أفراد عائلةِ المريض من دونِ الحصولِ على موافقةِ المريض، مما شكّلَ انتهاكاً لحقوقِ الخصوصيَّةِ وحمايةِ البيانات ، و يجبُ على الطبيب أن يحصلَ على موافقة المريض قبل مشاركة المعلومات الطبية مع الآخرين، حتى لو كانوا من أفراد الأسرة المقربين.

من المهم أن يحترم الأطباء والموظفون الطبيون سرية معلومات المرضى ، وأن يلتزموا بالأحكام القانونية المعمول بها لضمان خصوصية وحماية بيانات المرضى

الحالة الخامسة عشر :

زوجان مطلقان لديهما طفل قاصر ، يتلقى الطفل علاجاً طبيًّاً ، ويختلفُ الوالدان حول مشاركة المعلومات الطبية مع العاملين الطبيين الآخرين ، و يرغب الأب في مشاركة جميع المعلومات ذات الصلة مع الأطباء المعالجين، بينما تعتقد الأم أنَّهُ يجبُ مشاركةُ بعض البيانات فقط.

تكمن أهمية هذه الحالة في الصراع بين حقوق حاملي السلطة الوصيّة وحماية خصوصية الطفل. من المهم معاملة بيانات الطفل الطبية وفقًا للوائح الخصوصية المعمول بها، لضمان مراعاة مصالح الطفل وحقوق ومخاوف الوالدين بشكل مناسب.

الحل :

الحل لحالة الصراع بين حاملي السلطة الوصاية بشأن نقل بيانات طبية لطفل يمكن أن يكون كالتالي:

1ـ المادة 9 (2) (h) من اللائحة الأساسية لحماية البيانات :(DSGVO) تنصُّ هذه المادةُ على أنَّه يجوز معالجة فئات خاصة من البيانات الشخصية، ومن ضمنها البيانات الصحية، إذا كان ذلك في مصلحة عامة واتخذت تدابير مناسبة لحماية حقوق وحريات الأشخاص المعنيين. في هذه الحالة، يجب أن يكون نقل البيانات الطبية للطفل له أساس قانوني صحيح، مثل موافقة حامل السلطة الوصاية أو قرار قضائي.

2ـ قانون الشخصية المدنية :(BGB) ينظم قانون الشخصية المدنية السلطة الوصاية والمسؤولية الأبوية. خاصةً المواد 1626 وما يليها من قانون الشخصية المدنية تنص على أن كل من الوالدين لهما السلطة الوصاية المشتركة على الطفل ويجب أن يتخذا قرارات وفقًا لمصلحة الطفل. في حالة حدوث صراع بين الوالدين بشأن نقل بيانات طبية للطفل، يمكن اللجوء إلى الخدمة القضائية للطوارئ لاتخاذ قرار يخدم مصلحة الطفل ويتفق مع قوانين حماية البيانات.ـ

3ـ قانون حقوق المرضى :(Patientenrechtegesetz) ينظم هذا القانون حقوق المرضى، بما في ذلك حق السيطرة على المعلومات الشخصية وحماية الخصوصية. ينص على أنه يجوز نقل البيانات الطبية فقط بموافقة المريض أو في حالة وجود أساس قانوني.

في هذه الحالة، يجب على الوالدين، إذا لم يتم العثور على حل وسط، اللجوء إلى الخدمة القضائية للطوارئ لاتخاذ قرار يلبي مصلحة الطفل ويتوافق مع قوانين حماية البيانات. تساعد الخدمة القضائية للطوارئ بسبب كفاءتها القانونية وخبرتها في التعامل مع مثل هذه الحالات، على إيجاد حل مناسب.

الحالة السادسة عشر :

زوجان مفصولان يملكان طفلاً مشتركاً و يعيش الطفل مع الأم، في حين يحصل الأب على فترات زيارة منتظمة. يتلقى الطفل الفحوصات الطبية والعلاجات من طبيب محدد. عبرت الأم عن مخاوفها للطبيب بشأن إهمال الأب للطفل وعدم قيامه بواجباته الأبوية. ومع ذلك، يقرّرُ الطبيب بمبادرته الخاصة تبادل المعلومات الطبية والنتائج المفترضة لإهمال الطفل للأب، من دون أخذ موافقة صريحة من الأم.

الحل :

1- المادة 6 (1) من الدستور الألماني :(GG) تحمي هذه المادة حقوق الآباء ومصلحة الطفل. وتؤكد المسؤولية المشتركة لكل من الوالدين في تربية ورعاية الطفل وتطويره.

2- الفقرة 203 من قانون العقوبات :(StGB) تنظم هذه الفقرة من قانون العقوبات انتهاك الحياة الشخصية والخصوصية عن طريق الكشف غير المصرح به عن المعلومات. يمكن أن يُعتَبَر تبادل المعلومات الطبية للطفل من قبل الطبيب للوالد الآخر دون موافقة صريحة من الأم كانت مخالفة لحماية البيانات وسرية المعلومات.

3- الفقرة /203/ من قانون العقوبات أيضا :(StGB)تنظم هذه الفقرة انتهاك سرية المعلومات المهنية بواسطة الأطباء. يتعين على الأطباء الحفاظ على سرية المعلومات الطبية للمرضى وعدم نشرها إلا بموافقة صريحة أو في حالات استثنائية محددة قانونياً.

في هذه الحالة، قدم الطبيب المعالج بشكل غير مشروع معلومات طبية حساسة حول إهمال الطفل للوالد الآخر دون استصدار موافقة الأم. وهذا يشكل انتهاكًا لحقوق حماية البيانات وربما لسرية المعلومات المهنية للطبيب. في مثل هذه الحالات، من المهم أن يحترم الطبيب المعالج الخصوصية وحماية بيانات المرضى وأن يحصل على موافقة جميع الأطراف المعنية قبل تبادل المعلومات.

الحالة السابعة عشر :

في إحدى العيادات، يُعيَّنُ طبيب مستقل (Honorararzt) لفترة محدودة للمساعدة في علاج المرضى. و يُمنَحُ الطبيبُ المستقلُّ حقَّ الوصولِ إلى نظام الملفات الإلكترونية للمرضى في العيادة للوصول إلى المعلومات الطبية اللازمة لعمله ، ولكن بسبب خطأ في صلاحيات الوصول للنظام، يتمتع الطبيب المستقل بحق الوصول غير المحدود إلى جميع بيانات المرضى، بغض النظر عما إذا كانت ذات صلة بعمله أم لا.

الحل :

يشكل الوصول غير المقيد للبيانات الخاصة بالمرضى من قبل طبيب متعاقد انتهاكًا للخصوصية ويتعارض مع المواد القانونية التالية ذات الصلة دون تكرار الحالة:

1ـ المادة 5 (1) (a) من اللائحة الأساسية لحماية البيانات :(DSGVO) يجب أن يتم معالجة البيانات الشخصية بشكل قانوني ومشروع وشفاف

2ـ المادة 9 (1) من اللائحة الأساسية لحماية البيانات :(DSGVO) يعتبر معالجة فئات خاصة من البيانات الشخصية، بما في ذلك البيانات الصحية، محظورًا بشكل عام، ما لم يكن هناك موافقة صريحة من المعنيين أو أساس قانوني.

3ـ من قانون حماية البيانات الاتحادي :(BDSG) يجوز معالجة فئات خاصة من البيانات الشخصية، بما في ذلك البيانات الصحية، فقط في حالات محددة.

4ـ من قانون حماية البيانات الاتحادي :(BDSG) مبادئ معالجة البيانات الشخصية في سياق العمل، بما في ذلك مبدأ الغرض المحدد ومبدأ التقليل من البيانات.

5ـ من قانون حماية البيانات الاتحادي :(BDSG) المسؤولية ومعالجة البيانات بناءً على الطلب في قطاع الرعاية الصحية، بما في ذلك التزام الأمان المناسب للبيانات والامتثال لمتطلبات حماية البيانات.

6ـ من قانون العقوبات الألماني :(StGB) انتهاك الأسرار الخاصة عند الكشف غير المصرح به عن المعلومات الشخصية أو السرية.

7ـ الفقرة الأولى من المادة 7 لقانون منتجات الطبية:(MPG)

تنص هذه الفقرة على حماية بيانات المرضى فيما يتعلق بالأجهزة والمنتجات الطبية. إذ يعتبر الوصول غير المحدود للطبيب المستقل إلى جميع بيانات المرضى انتهاكًا لمتطلبات الأمان المنصوص عليها في قانون منتجات الطبية.

يعد الوصول الغير محدود للطبيب المستقل إلى جميع بيانات المرضى خرقًا للمتطلبات الأمنية المحددة في قانون منتجات الطبية. حيث يهدف هذا القانون إلى ضمان أن يتم تصميم واستخدام المنتجات الطبية وفقًا لمعايير السلامة والأمان، بما في ذلك حماية خصوصية بيانات المرضى.

من الأهمية بمكان أن تلتزم جميع الأطراف المعنية، بما في ذلك الطبيب المتعاقد والمؤسسة التي يعمل بها، بتوجيهات حماية البيانات واتخاذ التدابير المناسبة للتحكم في والحد من الوصول إلى بيانات المرضى. ويشمل ذلك تحديد حقوق الوصول بوضوح، وتدريب الموظفين فيما يتعلق بحماية البيانات، وتنفيذ تدابير الأمان لمنع الوصول غير المصرح به.

الحالة الثامنة عشر :

أحمد، الَّذي لا يجيدُ اللغة الرسمية بطلاقة ، يذهبُ لزيارةِ الطبيبِ لمناقشةِ مشاكِلِه الصحيَّة ، فيلاحظ الطبيب وجود صعوبة في التواصل ويقرر استدعاء مترجم لتسهيل الحديث الطبي.

أثناء الزيارة الطبية، يشارك المترجم في المحادثة للترجمة بين الطبيب وأحمد. وبذلك يكون المترجم قد حصل على وصول إلى المعلومات الطبية السرية بخصوص حالة صحة أحمد وأعراضه والتشخيصات المحتملة.

ومع ذلك، يلاحظُ أحمد أنَّ المترجمَ تحدث عن معلوماته الطبيَّةِ في محادثةٍ خاصَّة مع شخصٍ آخر بعد الجلسة الطبية ، و يشعر أحمد بالقلق بشأن تسريب معلوماته السرية إلى أطراف ثالثة وانتهاك خصوصيته وحماية بياناته الطبية.

الحل :

إذا قمنا بتوجيه بيانات طبية إلى مترجم خارج الحوار الطبي، وذلك بدون اتخاذ تدابير الحماية اللازمة للبيانات، يمكن أن يكون هذا تعدّياً على عدة قوانين لحماية البيانات ، و يمكن أن يكون من بين الفقرات القانونية المعنية بهذا الصدد ما يلي :

1- المادة /9/ من قانون حماية البيانات العامة في الاتحاد الأوروبي :(DSGVO) تنظّمُ هذه المادة حماية الفئات الخاصَّة من البيانات الشخصية ، والَّتي تشملُ بيانات الصحة ، و يُسمح بتبادل هذه البيانات الحسَّاسة مع أطراف ثالثة وفقًا لشروط محددة موضوعة في.DSGVO

2- المادة /203/ من قانون العقوبات الألماني :(StGB) تنصُّ هذه المادة على حماية الأسرارِ الخاصّةِ، والَّتي تشملُ المعلوماتِ الطبيَّة ، و قد يُعدُّ تبادلُ أو كشف بيانات المرضى لأطراف ثالثة بدون إذن صحيح عملاً جنائيًّاً .

3- المادة /5/ من قانون حماية البيانات الألماني :(BDSG) تنظم هذه المادة مبادئ معالجة البيانات في مجال الرعاية الصحية. تنص على أنه يجب معالجة البيانات الشخصية بطرق قانونية وباحترام حقوق الخصوصية.

4- المادة/ 9 / ، الفقرة 1 من قانون حماية البيانات الصحية في قطاع الرعاية الصحية :(GDSG) تتناول هذه المادة حماية بيانات الصحة وتضع الالتزام بالسرية وسلامة المعلومات كمتطلب أساسي.

5- المادة /11/ من قانونِ الأطبَّاء الفيدرالي :(BÄO) تنظّمُ هذه المادة سريَّةَ الطبيبِ ، إذ يلتزم الأطباء بالحفاظ على سرية جميع المعلومات الطبية التي تُوكَلُ إليهم ، يُسمح بإفشاء بيانات المرضى للغير ، مثل المترجم، فقط بشروط محددة ويجبُ أن يجري ذلك في مصلحةِ المريضِ وبمراعاة حماية البيانات.

تهدف الفقرات القانونية المذكورة إلى ضمان حماية مناسبة وسرية البيانات الطبية ، و يعدُّ الامتثالُ لهذه الأحكام أمراُ حاسماً للحفاظ على خصوصية المرضى وبناء الثقة في التعامل مع المعلومات الطبية الحساسة.

الحالة التاسعة عشر :

في إحدى المستشفيات، يُحتَفظُ بالسجلَّاتِ الطبيَّةِ والوثائق بانتظامٍ لتوثيقِ تاريخِ علاجِ المرضى ، و بعد انتهاءِ مدَّةِ الاحتفاظِ القانونيَّةِ ، يجبُ تدميرُ هذه الوثائق بشكلٍ سليمٍ لحمايةِ خصوصيَّةِ المرضى ، و في هذه الحالة حدثَ انتهاكٌ لحقوقِ الخصوصيَّةِ عندما ألقى أحد موظفي المستشفى بطريق الخطأ بالوثائقِ الطبيَّةِ السريَّةِ في حاويةِ ورقٍ عامَّة بدلاً من تدميرها بشكل آمن.

الحل :

إن التخلصَ غير السليم من المستندات الطبيَّةِ في مستشفى يشكّلُ انتهاكاً لحقوق الخصوصيَّةِ والبياناتِ الشخصيَّة ، و الفقراتُ التشريعية ذاتُ الصلة هي كالتالي:

1ـ المادة /32/ من قوانينِ حمايةِ البياناتِ العامَّةِ في الاتّحادِ الأوروبي :(GDPR) تنظّمُ هذه المادة أمان معالجة البيانات الشخصيَّة ، و يجبُ على المستشفيات اتّخاذُ تدابير تقنيَّة وتنظيميَّة مناسبةٍ لضمانِ سريَّة وسلامةِ البيانات، بما في ذلك التخلص الآمن من المستندات.

2ـ الفقرة 9 في قانون حماية البيانات الألماني :(BDSG) تحدد هذه الفقرة الالتزامات المتعلقة بأمان معالجة البيانات وتتطلب اتخاذ تدابير تقنية وتنظيمية مناسبة لضمان الحماية المناسبة للبيانات الشخصية.

3ـ قوانين المستشفيات الولاية: قد يتم تحديد قواعد ولاية خاصة بالمستندات الطبية وتخزينها والتخلص منها في قوانين المستشفيات لكل ولاية. تختلف هذه القوانين حسب الولاية.

و من المهم أن تلتزم المستشفيات بتطبيق قوانين حماية البيانات المعمول بها لضمان سرية وأمان بيانات المرضى. ويشمل ذلك التخلص السليم من المستندات لتجنب انتهاكات حقوق الخصوصية وحماية سرية المرضى.

الحالة العشرون :

موظَّفٌ في مؤسَّسةٍ طبيَّةٍ يمتلكُ صلاحيةَ الوصولِ إلى سجلَّاتِ المرضى الإلكترونيَّة يستغلُّ موقعَه للوصولِ غيرِ المصرَّحِ به إلى بياناتِ المرضى الطبيَّةِ ، يجمعُ معلوماتٍ حولَ التشخيصاتِ والعلاجاتِ والبياناتِ الصحيَّةِ الحسَّاسةِ من دونِ أن يكونَ ذلكَ ضروريَّاً لعملِه المهنيّ ، و يستخدمُ الموظَّفُ هذه البياناتِ لأغراضٍ شخصيَّةٍ أو قد يسلّمها لأطرافٍ ثالثةٍ ليس لديها مصلحةٌ مشروعةٌ في الحصولِ على هذه المعلومات .

في هذه الحالة، ينتهكُ الموظَّفُ قوانينَ حمايةِ البيانات، وخاصَّةً حمايةَ بياناتِ المرضى ، و يتصرَّفُ بنيَّةٍ خادعةٍ عن طريقِ الوصولِ إلى معلوماتٍ سريَّةٍ واستخدامها بشكلٍ سيّء ، و يمكن أن يكونَ لهذا السلوكِ آثارٌ خطيرةٌ على خصوصيَّةِ وحمايةِ بياناتِ المرضى المعنيين.

الحل :

-المادة /32/ من قانونِ حمايةِ البياناتِ العامَّة :(GDPR) تنظّمُ هذه المادَّةُ حمايةَ البياناتِ الشخصيَّةِ والتدابير الأمنيَّة الَّتي يجبُ على الشركاتِ اتّخاذُها لمنعِ فقدانِ البياناتِ أو سوءِ استخدامِها أو الوصولِ غيرِ المصرَّحِ به إليها.

-المادة /203/ من قانونِ العقوباتِ الألماني : (StGB) تنصُّ هذه المادَّةُ على انتهاكِ سريَّةِ الطبيبِ والمعالجِ ، و يمكنُ وصفُ اختراقِ بياناتٍ طبيَّةٍ من دونِ مصلحةٍ مشروعةٍ كانَتْ انتهاكاً لسريَّةِ المهنةِ.

-المادَّةُ /43/ من قانونِ حمايةِ البياناتِ الألماني : (BDSG) تنظّمُ هذه المادَّةُ حمايةَ البياناتِ الشخصيَّةِ عندَ معالجتِها من قبَلِ الكياناتِ غيرِ العامَّةِ ،و يمكنُ وصفُ اختراقِ بياناتٍ طبيَّةٍ انتهاكاً لأحكام.BDSG

- وفقاً للمادَّةِ /202 a/ من قانونِ العقوباتِ الألماني ، يُعدُّ جرمُ "اختراقِ البيانات" جريمةً جنائيَّةً ، تنصُّ المادَّةُ على حمايةِ البياناتِ وتحظرُ الوصولَ غيرَ المصرَّحِ به ، أو التجسّس غيرَ المصرَّحِ به ، أو استخدامَ البياناتِ غيرِ المصرَّحِ بها والَّتي تُحمَى من الوصولِ غيرِ المصرَّحِ به .

وتنصُّ المادَّةُ /202 a/ على أنَّ الشخصَ الَّذي يحصلُ بشكلٍ غيرِ مصرَّحٍ به على بياناتٍ ليست له ويتجسَّسُ عليها ، أو يحصلُ عليها بأيّ طريقةٍ غيرِ مصرَّح بها، قد يُعَاقَبُ بالسجنِ لمدّةٍ تصلُ إلى ثلاثِ سنواتٍ ، أو بغرامةٍ مالية.

و من المهمّ أنْ تَتَّخذَ المؤسَّساتُ الطبيَّةُ التدابيرَ الأمنيَّةَ المناسبةَ لمنعِ الوصولِ غيرِ المصرَّحِ به إلى بياناتِ المرضى ، وتجنّبِ انتهاكاتِ حمايةِ البيانات ، ويشملُ ذلكَ توعيةَ الموظّفينَ بقواعدِ حمايةِ البياناتِ ، وتنفيذَ آلياتِ المراقبةِ والتحكّمِ المناسبةِ ، وإجراءَ تدريباتٍ منتظمةٍ حولَ حمايةِ البياناتِ .

<u>انتهى بعونه تعالى</u>