Bezpieczeństwo informacyjne dotyczy podmiotu (człowieka lub organizacji, również takiej jak państwo), który może być zagrożony utratą zasobów informacyjnych lub otrzymaniem informacji złej jakości. *Bezpieczeństwo informacyjne* oznacza zatem uzasadnione zaufanie podmiotu do jakości i dostępności pozyskiwanej oraz wykorzystywanej informacji. Ale warunkiem bezpieczeństwa informacyjnego jest bezpieczna informacja, której definicja jest następująca:

Definicja 1.1
Bezpieczeństwo informacji oznacza *uzasadnione* (np. analizą ryzyka i przyjętymi metodami postępowania z ryzykiem) *zaufanie*, że nie zostaną poniesione straty wynikające z niepożądanej zmiany, na skutek realizacji zagrożenia, wymaganych wartości istotnych kryteriów jakości informacji.

Z powyższego wywodu wynika, że bezpieczeństwo informacji jest składową bezpieczeństwa informacyjnego – informację (dobrej jakości) najpierw trzeba pozyskać, a potem, w trakcie jej wykorzystywania przez podmiot, odpowiednio chronić. Kryteria jakości istotne dla poszczególnych kategorii informacji oraz konkretnych uwarunkowań jej przetwarzania zwykle określają, w przypadku organizacji biznesowej, w której takie informacje są przetwarzane i wykorzystywane, gremia kierownicze tej organizacji (podmiotu) przy pomocy odpowiednich służb. Należy także zauważyć, że bezpieczeństwo nie jest ani stanem, ani zdarzeniem, ani procesem – to imponderabilia z dziedziny psychologii, co swoje implikacje ma na przykład w możliwościach pomiaru bezpieczeństwa. Dokładniejsza dyskusja nad tym zagadnieniem jest przedstawiona w podrozdziale 2.9.

Ze względu na znaczenie dla podmiotu (w szczególności konkretnej osoby) wszystkie wykorzystywane przez niego i dotyczące go informacje można podzielić na *wrażliwe* i *niewrażliwe*. Informacje wrażliwe dla określonego podmiotu to te, które mogą zostać wykorzystane przeciwko jego interesom przez ujawnienie, uniedostępnienie oraz zmanipulowanie[6].

Do wrażliwych zaliczają się wszystkie informacje, które muszą być chronione, bo tak nakazują obowiązujące przepisy prawne[7]. Informacjami wrażliwymi są też takie, których nakaz ochrony nie jest zawarty w żadnych regulacjach prawnych, a które organizacjom je wytwarzającym i przetwarzającym są zwykle wskazywane przez kompetentne organy, na przykład służby ochrony państwa, wewnętrzne komórki bezpieczeństwa w danej organizacji, pełnomocnika ds. bezpieczeństwa informacji. Takimi informacjami mogą też być dane same w sobie niewrażliwe, ale które stają się takimi w powiązaniu z innymi informacjami, pozwalając wyciągnąć prawidłowe wnioski na przykład o strategii rynkowej firmy w kolejnym kwartale.

---

[6] Należy zwrócić uwagę, że wprowadzone określenie *informacje wrażliwe* ma szerszy zakres niż takie samo określenie stosowane zwyczajowo do informacji wymienionych w art. 27 *Ustawy o ochronie danych osobowych* [29] i o których w tym samym kontekście mówi p. 51 Rozporządzenia UE [21].

[7] Na przykład *Ustawa o ochronie danych osobowych*, *Ustawa o ochronie informacji niejawnych* oraz przepisy, w których zdefiniowano tzw. tajemnice, np. tajemnicę przedsiębiorstwa.

Identyfikacja informacji wrażliwej najczęściej ogranicza się do jej inwentaryzacji i przeglądu zasobów w ramach analizy ryzyka. Rzadko bierze się pod uwagę, że oprócz identyfikacji informacji wrażliwych w organizacji trzeba je zlokalizować także poza nią oraz uwzględnić informacje pośrednie, pozwalające na wnioskowanie. Powinno się także zidentyfikować obieg informacji wrażliwej – to pozwala m.in. na opracowanie procedury lokalizacji jej wycieków.

Dodatkowo sprawę komplikuje fakt, że:

- prawa własności w przypadku informacji są często trudne do określenia;
- ustalenie wartości strat w przypadku ataków informacyjnych bywa trudne lub wręcz niemożliwe – dotyczy to na przykład utraty spodziewanych korzyści, wizerunku, przewagi konkurencyjnej itp.[8];
- lokalizacja wartościowych informacji bywa trudna.

Podsumowując, *osoby odpowiedzialne za ochronę informacji powinny dbać o ochronę informacji wrażliwych, a nie danych osobowych czy informacji niejawnych*. Te kategorie informacji są tylko szczególnymi przypadkami informacji wrażliwej. Brak takiego podejścia do ochrony informacji jest podstawowym błędem organizacyjnym, którego nie zniwelują żadne środki techniczne.

Specjaliści od techniki komputerowej posługują się najczęściej pojęciem danych, a nie informacji. Przyjmuje się, że informacje jako przedmiot przetwarzania w systemach informatycznych nazywa się danymi. Jednak dla skutecznej ochrony danych/informacji, ze względu na przedstawione wcześniej zależności między systemem informacyjnym a informatycznym, ciągle aktualny paradygmat w dziedzinie bezpieczeństwa informacyjnego brzmi: *chronimy informacje – dane są tylko ich szczególnym przypadkiem.*

1.1. Prywatność, anonimowość, poufność, ...

Wymienione w tytule pojęcia dotyczą osób (podmiotów), o których informacja jest przetwarzana w systemach informacyjnych i najczęściej pojawiają się w powiązaniu z tzw. *danymi osobowymi* (w rozumieniu ustawy [29]). Maj 2018 roku to graniczny termin wprowadzenia do polskiego prawa Rozporządzenia [21] i Dyrektywy [22] – przepisów unijnych związanych z ochroną danych osobowych. Podczas opracowywania wspomnianych przepisów pojawiły się koncepcje *privacy by design* i *privacy by default*, ale dostrzeżono, że ustanawiane przepisy dotyczą ochrony danych osobowych, a nie prywatności i ostatecznie opisano to jako *data protection by design and by default*, czyli bez użycia słowa prywatność[9]. Jednak w trakcie różnych dyskusji, szkoleń i konferencji ww. nazwy koncepcji są powszechnie używane i mówi się o ochronie prywatności czy zapewnianiu prywatności. W kontekście tych wypowiedzi pojawiają się też często takie

[8] Czasami jednak może być oczywiste, np. po oszustwie, szantażu lub przelaniu środków z konta organizacji.

[9] W polskiej wersji przetłumaczone jako *Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych* (art. 25 Rozporządzenia [21]).