

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-ND 4.0 International) license
<https://creativecommons.org/licenses/by-nd/4.0>



p-ISSN 0551-911X, e-ISSN 2353-8104

Received: 19 May 2026

Revised: 29 May 2026

Accepted: 3 June 2026

Published: 28 September 2026

<https://doi.org/10.21697/pk.2026.69.3.04>

KINGA KARSTEN

Uniwersytet Papieski Jana Pawła II w Krakowie

kinga.karsten@upjp2.edu.pl

<https://orcid.org/0000-0001-6244-8650>

PRZETWARZANIE DANYCH W FORMIE CYFROWEJ PRZEZ PODMIOTY KOŚCIELNE – POSTULATY *DE LEGE LATA* I *DE LEGE FERENDA*

Treść: Wstęp; 1. Regulacje dotyczące przetwarzania danych w Kościele katolickim w Polsce; 1.1. Podstawy autonomicznego porządku w obszarze ochrony danych; 1.2. Regulacje dotyczące przetwarzania w obszarze administracyjnym; 2. Uzupełnienie luki prawnej w obszarze cyfrowego przetwarzania danych; 2.1. Normy kan. 19; 2.2. *Analogia legis*; 2.3. *Analogia iuris*; 2.4. Orzecznictwo i praktyka Kurii Rzymskiej oraz opinia doktryny kanonistycznej; 3. Postulaty; 3.1. Postulaty *de lege lata*; 3.2. Postulaty *de lege ferenda*; Podsumowanie

Wstęp

Podmioty kościelne, takie jak diecezje, zakony, parafie coraz częściej sięgają po cyfrowe (elektroniczne) narzędzia w celu przetwarzania danych, w tym danych osobowych. Narzędzia te są wprowadzane w tych jednostkach zazwyczaj oddolnie, a niekiedy odgórnie – na polecenie władzy kościelnej. Narzędzia te to przykładowo aplikacja „mKsiądz” – aplikacja umożliwiająca m.in. korzystanie z cyfrowej wersji legitymacji kapłańskiej oraz mobilnej wersji „Systemu Synodi”. „System Synodi” to z kolei rozbudowany system e-usług dla Kościoła katolickiego, składający się z wielu modułów, pozwalający na przetwarzanie danych osobowych znacznej liczby wiernych. Inna aplikacja to „Fara” – oprogramowanie dla parafii obejmujące moduły:

Kartoteka, Jubilaci, Statystyka, Odwiedziny chorych, Trasy kolędowe i inne. Wymagania techniczne i środowiska działania omawianego oprogramowania są niejednorodne – rozciągają się od rozwiązań chmurowych o wysokich wymaganiach, aż po scenariusze, w których dane pozostają i są przetwarzane w całości na komputerze lub w wewnętrznej sieci.

Te narzędzia funkcjonują bez wyraźnie ustalonego statusu i ram. W systemie prawnym Kościoła katolickiego w Polsce brak jest bowiem aktu normatywnego regulującego cyfrowe przetwarzanie danych. Szczątkowe regulacje dotyczące cyfrowego przetwarzania danych zawarte w art. 10, art. 23 ust. 3 i art. 25 Dekretu Konferencji Episkopatu Polski z 2018 r. są niewystarczające (Sobiecka 2025, 291). Ten brak regulacji w zakresie cyfrowego przetwarzania danych jest poważną praktyczną trudnością dla administratorów oraz może generować ryzyko dla bezpieczeństwa danych osobowych.

Należy w tym miejscu wyraźnie odróżnić dwie płaszczyzny. Pierwsza to ochrona danych osobowych uregulowana co do zasady przez technicznie neutralny Dekret KEP z 2018 r., który stosuje się do każdej formy przetwarzania, w tym formy cyfrowej. Druga to kancelaryjno-administracyjne przepisy regulujące np. cyfrowe prowadzenie dokumentacji, obieg dokumentów oraz archiwizację. Luka prawna dotyczy wyłącznie tej drugiej płaszczyzny. Brakuje przykładowo kościelnego aktu normatywnego, który określałby rygory cyfrowego prowadzenia ksiąg parafialnych i innych rejestrów kościelnych, stanowiąc tym samym elektroniczny odpowiednik *Przepisów o prowadzeniu ksiąg parafialnych: ochrzczonych, bierzmowanych, małżeństw i zmarłych, oraz księgi stanu dusz* z 1947 r., które wydała Konferencja Episkopatu Polski.

W artykule tym zostanie pokazane na przykładach, jak tę lukę wypełnić. Będą sformułowane także postulaty *de lege lata* i *de lege ferenda* dotyczące cyfrowego przetwarzania danych przez podmioty kościelne.

1. Regulacje dotyczące przetwarzania danych w Kościele katolickim w Polsce

1.1. Podstawy autonomicznego porządku w obszarze ochrony danych

Na gruncie prawa powszechnie obowiązującego (prawa świeckiego), podstawą prawną do autonomicznego porządku w obszarze ochrony danych w Kościele katolickim, zresztą tak samo jak i w innych związkach wyznaniowych, jest RODO (Rozporządzenie 2016/679). Rozporządzenie to w art. 91 daje możliwość stosowania przez te podmioty, wewnętrznych przepisów ochrony danych osobowych, co łączy się z wyłączeniem tych podmiotów z bezpośredniego stosowania przepisów RODO w ich obszarze statutowym (czysto kościelnym czy religijnym). RODO pozostaje jedynie punktem odniesienia i standardem minimalnym dla procesów przetwarzania danych w związkach wyznaniowych.

Przywołany artykuł RODO obwarował wyłączenie spod jednolitej ochrony danych kilkoma przesłankami. Kościół katolicki w Polsce spełnił te wymagania, czyli: 1. posiada prawny status kościoła w systemie prawa krajowego (polskiego); 2. stosował w momencie wejścia w życie RODO, czyli 24 maja 2016 r., szczegółowe zasady ochrony osób fizycznych w związku z przetwarzaniem oraz 3. dostosował własne dotychczasowe zasady ochrony danych osobowych do RODO (Krocze 2020, 37-48).

W celu realizacji tej ostatniej z wymienionych przesłanek system ochrony danych w Kościele katolickim został zorganizowany na podstawie przepisów Kodeksu Prawa Kanonicznego z 1983, Dekretu KEP z 2018 r., a także Przepisów z 1947 r. Między innymi te źródła norm wymienia w preambule wspomniany Dekret KEP z 2018 r. – zapewne dla wykazania realizacji tej przesłanki. Wskazane regulacje mogą być, zgodnie z art. 2. Dekretu KEP z 2018 r., uzupełniane przez akty normatywne prawa partykularnego (diecezjalnego lub zakonnego), czyli dekrety ogólne „za pomocą których właściwy ustawodawca wprowadza dla wspólnoty zdatnej do przyjęcia ustawy przepisy obowiązujące wszystkich” (kan. 29).

Dla praktyki przetwarzania danych w podmiotach kościelnych mają znaczenie także inne dokumenty, m.in. praktyczne wskazania i okólniki wydawane przez kościelny organ nadzoru, czyli Kościelnego Inspektora Ochrony Danych (KIOD) oraz wewnętrzne instrukcje, polityki i zarządzenia wydawane przez administratorów, zwykle pełniących jakiś urząd kościelny – jak biskupi diecezjalni czy inni ordynariusze (kan. 134 § 1–§2).

1.2. Regulacje dotyczące przetwarzania w obszarze administracyjnym

Będący głównym źródłem norm w obszarze ochrony danych Dekret KEP z 2018 r. jest właściwie okrojona kopia RODO. W rezultacie Dekret KEP z 2018 r. jest co do zasady, jak to już wskazano – neutralny pod względem technicznym. Tę neutralność odzwierciedla motyw 15 RODO oraz art. 24 ust. 1 RODO, znajdujący swój odpowiednik w art. 17 ust. 1 Dekretu KEP z 2018 r., a także art. 32 ust. 1 RODO i art. 22 ust. 1 Dekretu KEP z 2018 r. Oznacza to, że zgodnie z ogólną zasadą, to na administratorze w Kościele spoczywa odpowiedzialność za właściwy dobór środków technicznych i organizacyjnych w czasie przetwarzania danych, niezależnie od tego, czy dane przetwarza w sposób tradycyjny, czy cyfrowy – art. 17 ust. 1 Dekretu KEP z 2018 r.

Pewne niewielkie wyjątki od reguły neutralności technicznej są wprawdzie zawarte np. w art. 25 Dekretu KEP z 2018 r., który stanowi o przechowywaniu danych w archiwach cyfrowych. Jest to regulacja bardzo ogólna i dotycząca wyłącznie *verba legis*: „archiwów cyfrowych”, a nie przetwarzania danych w formie elektronicznej w innych procesach, czyli dla innych, to jest niearchiwalnych celów.

Napisano już we wstępie, że w obecnym stanie prawnym nie istnieje kościelny akt normatywny, wiążący wszystkie podmioty Kościoła katolickiego w Polsce, który wprost ustanawiałby podstawy prawne przetwarzania danych osobowych w formie cyfrowej. Diecezje czy zakony, a także ich jednostki organizacyjne mogą posiadać własne regulacje dotyczące elektronicznego przetwarzania danych.

Przykładem takiego rozwiązania jest wydana przez biskupa diecezjalnego archidiecezji wrocławskiej *Instrukcja dotycząca prowadzenia kartoteki parafialnej* z dnia 22 października 2018 r. Zaznaczyć trzeba,

że pomimo błędnego terminu prawnego w tytule – „instrukcja” (zob. kan. 34 § 1) i wadliwej techniki legislacyjnej, np. ostatnie zdanie tego dokumentu zawiera treść normatywną, lecz znajduje się poza częścią artykułową, a więc powinno być ono zawarte w jednostce redakcyjnej aktu normatywnego – jest to dekret ogólny (ustawa kościelna). W tym dekrete określono „Kartotekę parafialną” jako „zbiór danych osobowych wiernych przynależących do parafii”. Zbiór ten można prowadzić „w formie elektronicznej z zachowaniem szczegółowych norm bezpieczeństwa w przestrzeni cyfrowej” (AW, 2018, art. 1 § 2). Jednakże, aby „przetwarzać dane parafian tylko w formie elektronicznej, należy posiadać pisemną zgodę ordynariusza miejsca” (AW, 2018, art. 1 § 3). Należy przyjąć, że inne regulacje dotyczące kartoteki w formie papierowej, które zawiera omawiana Instrukcja, trzeba stosować odpowiednio w przypadku kartoteki prowadzonej elektronicznie.

W działalności podmiotów kościelnych są także wydawane opracowania o charakterze praktycznym, które jako wytyczne, rekomendacje, dobre praktyki (*soft law*) mogą być pomocne w działalności administratorów. Przykładem próby takiego wdrożenia regulacji ochrony danych osobowych w strukturach kościelnych jest *Przewodnik po nowych przepisach dotyczących ochrony danych osobowych dla osób pełniących posługę w Kościele katolickim na terytorium Polski (stan prawny na dzień 25 maja 2018 roku). Materiały pomocnicze przygotowane dla uczestników szkolenia w Archidiecezji Lubelskiej*. Dokument ten, choć pozbawiony waloru normatywnego, stanowi doniosłe źródło interpretacyjne, ukazujące sposób, w jaki autorzy tego dokumentu rozumieli i chcieli wdrożyć nowe obowiązki wynikające z Dekretu KEP z 2018 r. i RODO.

Chcąc przybliżyć ten dokument, należy omówić odpowiedź na pytanie nr 16 o brzmieniu: „Czy wolno przechowywać i przetwarzać dane w formie elektronicznej?”. Wskazano w nim, że: „Wolno przechowywać i przetwarzać dane w formie elektronicznej, z zastrzeżeniem pełnej ochrony tych danych”. Sformułowanie to budzi poważne wątpliwości z perspektywy metodologicznej. Wskazówka ta ma bowiem charakter ogólnikowy. Zawiera ona wprowadzić dwie reguły: 1. zezwolenie na przetwarzanie elektroniczne oraz 2. wyznaczenie

standardu ochrony, jednak żadnej z nich nie precyzuje w sposób operacyjny, czyli praktycznie wykonalny i dostatecznie precyzyjnie opisany. Pojęcie „pełnej ochrony danych” nie zostało zdefiniowane ani odniesione do konkretnych mechanizmów technicznych lub organizacyjnych. W efekcie wskazówka pozostaje postulatem – nie przekazuje wiedzy o tym, jakie środki należy wdrożyć, by spełnić wymagany standard. Ta ogólnikowość stwarza ryzyko, iż podmiot może uznać, że wypełnił obowiązek ochrony, nie podejmując żadnych konkretnych działań techniczno-organizacyjnych nawet w obiektywnie minimalnym zakresie.

O ile techniczna neutralność ustaw regulujących ochronę danych w działaniu Kościoła, czyli Dekretu KEP z 2018 r. i RODO, ma swoje uzasadnienie w dążeniu do przerzucenia odpowiedzialności na administratora w sytuacji szybkich zmian technologicznych, to publikacje o charakterze przywołanego Przewodnika powinny wypełniać tę zamierzoną lukę konkretem. Ich funkcja polega bowiem nie na powielaniu ogólnych zasad z ustaw, lecz na ich operacjonalizacji, czyli wskazywaniu możliwych do wdrożenia standardów postępowania. Przewodnik, który w odpowiedzi na pytanie o dopuszczalność przetwarzania elektronicznego poprzestaje na sformułowaniu „pełna ochrona danych”, nie realizuje swojej funkcji.

Bardziej szczegółowe wskazówki, inspirowane technicznymi realiami przetwarzania danych, zawiera w Przewodniku odpowiedź na pytanie nr 17: „Jakie wymagania winny spełniać komputer i oprogramowanie używane do przechowywania danych osobowych?” Sformułowano w tym zakresie dziewięć zaleceń, z których dla poruszanых w tym artykule kwestii najważniejsze to: „3) Komputer, na którym są przechowywane dane osobowe, może mieć zainstalowane wyłącznie oprogramowanie legalne i wyłącznie takie, które służy do gromadzenia i przetwarzania danych. 4) Dostęp do komputera winien być zabezpieczony hasłem o odpowiednim stopniu skomplikowania, które powinno być odpowiednio często zmieniane, jak również nie należy korzystać z opcji zapamiętywania hasła. 5) Dostęp do oprogramowania, przy pomocy którego są gromadzone i przetwarzane dane osobowe, winien być zabezpieczony odrębnym hasłem. 6) Z zasady

na tym komputerze nie powinny być instalowane komunikatory ani inne programy, które powodują ryzyko dostępu osób nieuprawnionych za pomocą sieci komputerowej. 7) Zaleca się, aby komputer ten nie był na stałe podłączony do sieci internet. 8) Komputer winien być zabezpieczony przy użyciu aktualnego odpowiedniego oprogramowania (w tym program antywirusowy)". Zalecenia te, choć praktycznie użyteczne, mają charakter nadmiernie kazuistyczny i technologicznie zdezaktualizowany już 2018 r., czyli roku wydania Poradnika. Odzwierciedlają one podejście charakterystyczne dla wcześniejszego etapu cyfryzacji, pomijając współczesny model bezpieczeństwa oparty na zarządzaniu ryzykiem, szyfrowaniu danych, wieloskładnikowym uwierzytelnianiu oraz bezpieczeństwie usług chmurowych.

Przewodnik podaje także w odpowiedzi na pytanie nr 18, że „Wolno wykonywać kopie zbiorów danych, pod warunkiem właściwego zabezpieczenia tych kopii, o ile to możliwe przy pomocy odpowiedniego oprogramowania. Nośniki z kopiami zbiorów danych (np. dyski przenośne) muszą być przechowywane przy zastosowaniu takich samych zasad jak przy przechowywaniu ksiąg parafialnych". Odnotować należy odwołanie do zasad przechowywania ksiąg parafialnych. Jest to zabieg, który ujawnia pewną łączność między tradycyjnymi formami archiwizacji a wymogami nowoczesnego bezpieczeństwa informatycznego. Księgi parafialne chronione są przed zagrożeniami fizycznymi, np. zniszczeniem, kradzieżą, nieuprawnionym wglądem poprzez zamknięcie w odpowiednich pomieszczeniach o ograniczonym dostępie. Tymczasem nośniki cyfrowe narażone są na jakościowo odmienny katalog zagrożeń, do którego należą m.in. złośliwe oprogramowanie, nieautoryzowany zdalny dostęp, podatności kryptograficzne, a także ryzyko nieodwracalnej utraty danych wskutek awarii sprzętu. Analogia do ksiąg parafialnych, choć zrozumiała i obliczona na oswojenie adresata Poradnika z nową problematyką poprzez odwołanie do dobrze znanych mu praktyk, jest zatem strukturalnie nieadekwatna. Fizyczne zabezpieczenie nośnika nie zastępuje jego szyfrowania, a zasada ograniczonego dostępu do pomieszczenia nie eliminuje ryzyka zdalnego przełamania zabezpieczeń systemowych.

2. Uzupełnienie luki prawnej w obszarze cyfrowego przetwarzania danych

2.1. Normy kan. 19

Brak stosownych regulacji tworzy lukę prawną (*lacuna legis*). W celu jej uzupełnienia należy skorzystać z kan. 19, który mówi: „Jeżeli w danej materii brak wyraźnego przepisu ustawy powszechnej lub partykularnej albo prawa zwyczajowego, sprawa – z wyjątkiem karnej – powinna być rozstrzygnięta z uwzględnieniem ustaw wydanych w podobnych sprawach, ogólnych zasad prawa stosowanych z zachowaniem słuszności kanonicznej, orzecznictwa i praktyki Kurii Rzymskiej oraz powszechnej i stałej opinii uczonych”. Ustawodawca wskazał więc na kilka źródeł uzupełnienia luki. Są to źródła równorzędne (Pawluk 1985, 232; Szafrowski 1985, 159). Do usunięcia luki prawnej można użyć tylu źródeł, ile potrzeba (Kroczek, 2004, 40). W praktyce, źródła, z których można skorzystać do uzupełnienia luki prawnej to, po pierwsze, ustawy kościelne wydane w podobnych sprawach, co stanowi zastosowanie (1) *Analogia legis*. Po drugie, ogólne zasady prawa kanonicznego stosowane z zachowaniem słuszności kanonicznej, czyli chodzi tu o (2) *Analogia iuris*, której przesłanką jest założenie, że prawo kanoniczne stanowi spójnie logiczny system powiązanych zasad. Po trzecie, uzupełnienia norm można dokonać przez odwołanie się do (3) praktyki kompetentnych w danym obszarze spraw organów i orzecznictwa oraz doktryny kanonistycznej.

2.2. *Analogia legis*

Dekret KEP z 2018 r. i Przepisy z 1947 r. to ustawy, które należy wykorzystać jako pierwsze źródła uzupełnienia luki prawnej, gdyż zawierają one przepisy przedmiotowo obejmujące ten sam przedmiot – dane osobowe.

Stosowanie analogii z tych ustaw nie oznacza, iż przepisy stanowiące podstawę analogii mają być zastosowane dosłownie. Dokonać się to powinno w drodze „odpowiedniego stosowania”, co oznacza, że niektóre przepisy stosuje się wprost, bez modyfikacji, niektóre dostosowuje do stanu faktycznego lub do charakteru

rozpoznawanej sprawy, a niektóre przepisy się pomija (Morawski 2010, 230–231).

Wprost i bez zmian zastosować można art. 17 ust. 1 i ust. 3 Dekretu KEP z 2018 r. w zakresie obowiązków administratora. Zgodnie z art. 17 ust. 1 Dekretu KEP z 2018 r. Administrator powinien wdrożyć odpowiednie środki techniczne i organizacyjne w celu ochrony danych, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych. W odniesieniu do cyfrowych systemów zarządzania danymi w kancelarii parafialnej, takich jak programy FARA czy System Synodi, realizacja powyższego obowiązku sprowadza się do wdrożenia znanych z innych obszarów wykorzystania przetwarzania elektronicznego danych zabezpieczeń informatycznych.

Przykładowo, administrator danych jest zobligowany do zapewnienia procedur dostępu np. poprzez zindywidualizowane konta dla każdego z użytkowników systemu (np. wikariuszy, pracowników świeckich), wymuszania stosowania haseł o odpowiednim standardzie bezpieczeństwa oraz środków technicznych minimalizującym ryzyko utraty integralności i dostępności danych z ksiąg metrykalnych, takich jak cykliczne tworzenie szyfrowanych kopii zapasowych bazy danych czy też stosowanie aktualnego oprogramowania zabezpieczającego. Szczegóły, z racji neutralności technicznej prawa, w tym zakresie pozostawia się administratorowi.

Z kolei w art. 17 ust. 3 Dekretu KEP z 2018 r. wyrażony został nakaz, aby na etapie projektowania, a także w trakcie samych procesów przetwarzania, zastosować odpowiednie środki techniczne i organizacyjne, służące ochronie danych. Oznaczać to może w przypadku przetwarzania elektronicznego z wykorzystaniem oprogramowania wymóg doboru i konfiguracji takich narzędzi, które architektonicznie implementują zasady ochrony danych (tzw. zasada *data protection by design*). W praktyce przejawia się to w stosowaniu mechanizmów kontroli dostępu opartych na rolach, co ma gwarantować to, że np. osoba świecka obsługująca program nie ma wglądu do określonych adnotacji charakterze duszpasterskim, do których dostęp posiada wyłącznie duszpasterz. Wdrożeniem tej normy może być również

wbudowany w programie system logowania zdarzeń informatycznych, pozwalający na identyfikację podmiotu, który dokonał modyfikacji lub usunięcia konkretnych danych.

Innym przykładem dostosowania do formy cyfrowej przetwarzania istniejących przepisów może być realizacja norm nakazujących formę „pismenną” dokonania pewnych czynności, np. powiadomienia wnioskodawcy o dokonanej adnotacji dotyczącej danych tej osoby (Konferencja Episkopatu Polski 2018, art. 13 ust. 4; zob. także Konferencja Episkopatu Polski 2018, art. 12 ust. 2 i ust. 3). Opierając się na wykładni celowościowej przepisów zawierających ten nakaz oraz stosując *Analogia legis*, w kontekście zasad wykładni Dekretu KEP z 2018 r. zawartych w kan. 17, a szczególnie dyrektywy wykładni *in contextu* (Kroczek and Skonieczny 2022 49-63), możliwe jest poosłużenie się uregulowaną w Kodeksie cywilnym [kc, art. 77 (1) oraz art. 77 (2)] formą dokumentową, która wymaga utrwalenia oświadczenia woli w postaci dokumentu umożliwiającego ustalenie osoby składającego dane oświadczenie. Takie posiłkowe odwołanie do prawa świeckiego w zakresie form oświadczeń woli w celu uzupełnienia luki prawnej jest więc usprawiedliwione.

Wymogi stawiane przez obowiązujące prawo księgom parafialnym w tradycyjnym modelu rejestracji nie tracą swojej normatywnej doniosłości w erze cyfrowej. Jak wyżej wskazano, Przepisy z 1947 r., formułowały szczegółowe wymogi dotyczące materialnej i formalnej warstwy ewidencji parafialnej, których funkcjonalne odpowiedniki winny być odnalezione i wdrożone przez administratorów kościelnych systemów informatycznych.

Po pierwsze, trwałość nośnika i środka zapisu. Przepisy z 1947 r. (KEP 1947, pkt 4–5) nakazywały sporządzanie ksiąg z papieru, który ma być „trwały i jakościowo dobry”, oprawy księgi parafialnej, która ma być „trwała i mocna”, a wpisów dokonywać atramentem, „bardzo wyraźnie i starannie”. Te wskazania wyrażają zasadę trwałości i niezniszczalności zapisu kościelnego jako dokumentu publicznego w rozumieniu kan. 1813-1816 Kodeksu Prawa Kanonicznego z 1917 r. Przepisy z 1947 r. zostały wydane na podstawie tego kodeksu. Przenosząc ową zasadę na grunt elektroniczny, administrator zobowiązany

jest do wdrożenia systemów zapewniających ciągłość i integralność danych, np. poprzez zastosowanie nadmiarowych macierzy dyskowych (RAID), automatycznych kopii zapasowych przechowywanych w geograficznie odrębnych lokalizacjach (*offsite backup*) czy szyfrowanej archiwizacji w środowiskach chmurowych.

Po drugie, nienaruszalność i kontrola modyfikacji treści aktu. Przepisy z 1947 r. (KEP1947, pkt 5-6) bezwzględnie zakazywały wyškrobywania i przekreślania wpisów, a w razie omyłki nakazywały jedynie lekkie przekreślenie błędnego fragmentu z jednoczesnym wpisaniem tekstu właściwego, opatrzonym datą i własnoręcznym podpisem proboszcza. Regulacja ta realizowała kanoniczną zasadę autentyczności aktu publicznego, wykluczając jego zafałszowanie. W systemach informatycznych funkcjonalnym i ścisłym ekwiwalentem tej normy jest stosowanie niezmiennych, kryptograficznie zabezpieczonych dzienników audytowych, rejestrujących każdą operację na rekordzie metrykalnym: treść modyfikacji, znacznik czasowy oraz jednoznaczny identyfikator użytkownika. Mechanizm ten uniemożliwia dokonanie jakiegokolwiek korekty danych bez pozostawienia trwałego, weryfikowalnego śladu.

Po trzecie, ochrona przed dostępem osób nieuprawnionych. Zgodnie z pkt 9 Przepisów z 1947 r., księgi parafialne przechowywane być musiały w kancelarii, w zamkniętej szafie, tak aby „osoby obce nie miały do nich dostępu i by je uchronić przed zniszczeniem lub kradzieżą”. Norma ta odzwierciedla zasadę poufności i fizycznego bezpieczeństwa dokumentu kościelnego, którą dziś należy realizować przy użyciu adekwatnych środków technicznych, np. mechanizmów uwierzytelniania użytkowników, w tym wieloskładnikowego uwierzytelniania (*multi-factor authentication*), szyfrowania baz danych, a nadto modelu kontroli dostępu opartego na ściśle określonych rolach użytkowników systemu.

Po czwarte, przesyłanie danych. Przepisy z 1947 r. (pkt 3) nakładały na proboszcza obowiązek corocznego przesyłania drugiego egzemplarza ksiąg metrykalnych do kurii diecezjalnej za pośrednictwem dziekana, po wcześniejszym opatrzeniu go świadectwem proboszcza i indeksem alfabetycznym. Obowiązek ten, wyrażający zasadę

nadzoru kanonicznego nad księgami i znaczenia archiwizacji, winien być dziś wypełniany przez automatyczną, szyfrowaną replikację danych parafialnych z lokalnego serwera na zabezpieczone serwery archiwalne np. kurii diecezjalnej, z zachowaniem integralności kryptograficznej przesyłanych zbiorów i możliwością weryfikacji autentyczności replikacji po stronie odbiorczej.

2.3. *Analogia iuris*

Zastosowanie *Analogia iuris* w procesie uzupełniania luki prawnej na podstawie kan. 19 CIC/83 wymaga oderwania się od kazuistycznych rozwiązań technicznych i sięgnięcia do fundamentalnych wartości chronionych przez system prawa kanonicznego. W kontekście cyfryzacji ksiąg metrykalnych pierwszoplanowe znaczenie zyskuje zasada pewności obrotu prawnego. Ewidencja parafialna (księgi parafialne) nie jest bowiem wyłącznie zbiorem historycznym, lecz stanowi fundament ustalania statusu kanonicznego (głównie) wiernego, w tym przyjęcia chrztu (CIC/83, kan. 877 § 1), bierzmowania (CIC/83, kan. 535 § 2), zawarcia małżeństwa (CIC/83, kan. 535 § 2 i kan. 1122 § 1) czy przyjęcia święceń (CIC/83, kan. 535 § 2), przejścia do Kościoła *sui iuris* (CIC/83, kan. 112 § 3 i kan. 535 § 2), uzyskania reskryptu dyspensy (CIC/83, kan. 1706 i kan. 1081) oraz innych faktów mających kanoniczne znaczenie (Karsten 2021, 26-27).

Wymóg wiarygodności kościelnego aktu publicznego oznacza, że z ogólnej zasady pewności prawa wyprowadzić należy obowiązek zagwarantowania integralności i autentyczności zapisów elektronicznych. Administrator danych musi zatem implementować takie rozwiązania technologiczne, jak przykładowo zaawansowana kryptografia czy rozproszone, niezmiennie systemy archiwizacji, które w środowisku cyfrowym wyeliminują ryzyko nieodwracalnej utraty lub ukrytej modyfikacji danych sakramentalnych, gwarantując niezawodność tożsamą z fizyczną nienaruszalnością tradycyjnych ksiąg.

Powyższa reguła znajduje swoje ostateczne zakotwiczenie w nadrzędnej zasadzie całego porządku kanonicznego, jaką jest zbawienie dusz (*salus animarum suprema lex*), wyrażonej w kan. 1752 CIC/83. W erze społeczeństwa informacyjnego dbałość o duchowe dobro

wiernych nierozzerwalnie wiąże się z obowiązkiem ochrony ich prywatności oraz zapobieganiem sytuacjom, w których wyciek lub manipulacja wrażliwymi informacjami mogłyby wywołać zgorszenie, naruszyć dobre imię osoby lub wprost utrudnić jej dostęp do dóbr duchowych Kościoła.

Wywodząc zatem normę postępowania bezpośrednio z tej fundamentalnej zasady, należy uznać, że dla kościelnego administratora wdrożenie najwyższych standardów cyberbezpieczeństwa nie jest wyłącznie uciążliwym obowiązkiem administracyjnym o charakterze technicznym narzuconym przez świeckie lub kościelne organy nadzoru, lecz stanowi imperatyw o charakterze ściśle kanonicznym i duszpasterskim. Profesjonalne zabezpieczenie systemów informatycznych przed nieuprawnionym dostępem staje się w ten sposób prawnym wyrazem troski Kościoła o duchowe i prawne bezpieczeństwo członków swojej wspólnoty.

2.4. Orzecznictwo i praktyka Kurii Rzymskiej oraz opinia doktryny kanonistycznej

W zakresie omawianym w tym artykule, czyli w obszarze cyfrowego przetwarzania danych w Kościele w Polsce, niektóre ze źródeł pomagających uzupełnić lukę prawną są puste, np. orzecznictwo i praktyka Kurii Rzymskiej, czyli stały sposób załatwiania spraw na drodze sądowej lub administracyjnej przez jednostki organizacyjne Stolicy Apostolskiej. Stolica Apostolska nie wydała jeszcze żadnego rozstrzygnięcia w przedmiotowym obszarze.

W takiej sytuacji, trzymając się *ratio legis* tego przepisu, trzeba szukać innych zbliżonych źródeł, np. można powołać się na praktykę kościelnego organu nadzorczego w obszarze ochrony danych w Polsce, czyli KIOD.

Działalność KIOD dostarcza przykładów odnoszących się do przetwarzania danych w formie elektronicznej np. *Okólnik z dnia 20 grudnia 2023 r. dotyczący przetwarzania danych osobowych w systemach informatycznych*. KIOD wskazywał w nim na kluczowy element budowania systemu ochrony danych przetwarzanych w formie elektronicznej. Jest nim obowiązek administratora właściwego

i niezwłocznego włączania inspektora ochrony danych we wszystkie sprawy dotyczące ochrony danych osobowych (zob. KEP 2018, art. 31 ust. 1) oraz zapewnienie mu niezależnego działania (RODO, motyw 97; Karsten 2025, 5-6). „Ten obowiązek aktualizuje się na etapie planowania i projektowania procesów przetwarzania oraz ma szczególne znaczenie w przypadku procesów, które z racji uwarunkowań technicznych (np. przetwarzanie danych w Internecie) niosą poważne ryzyko dla bezpieczeństwa danych oraz dla praw i wolności osób, których dane dotyczą” (KIOD 2023). Jak wskazuje praktyka wielu diecezji czy zakonów w Polsce, ten element jest pomijany. Decyzje dotyczące wdrożenia elektronicznego przetwarzania danych podejmowane są przy uwzględnieniu argumentów na poziomie ekonomicznym, bez odnoszenia się do bezpieczeństwa danych.

Gdy zaś chodzi o stałą opinię uczonych, to kanonistyczna literatura przedmiotu w zakresie elektronicznego przetwarzania danych w Kościele jest bardzo niewielka i raczej poruszana na wystąpieniach naukowych lub szkoleniowych (Urząd Ochrony Danych Osobowych 2026). Jak to celnie zauważono: „nie można jeszcze mówić ani o powszechnej, ani o stałej polskiej nauce kanonistycznej w tym zakresie” (KroczeK and Skonieczny 2022, 60). W tym więc przypadku „poważnym argumentem w dyskursie kanonistycznym może być dorobek doktryny prawa świeckiego (KroczeK and Skonieczny 2022, 60). Z tego dorobku należy korzystać.

3. Postulaty

3.1. Postulaty *de lege lata*

Wnioski płynące z obecnego stanu prawnego opierają się na rozróżnieniu pomiędzy obowiązującymi przepisami o ochronie danych (KEP 2018) a odpowiednim stosowaniem przepisów kancelaryjnych (KEP 1947). Konsekwentne stosowanie tej dystynkcji pozwala na zabezpieczenie praw wiernych w oczekiwaniu na interwencję ustawodawcy.

De lege lata można sformułować kilka postulatów interpretacyjnych i praktycznych, które nie wymagają zmiany obowiązującego prawa, lecz jego konsekwentnego stosowania.

Po pierwsze, z uwagi na techniczną neutralność prawodawstwa kościelnego, każda elektroniczna baza danych, nawet ta o charakterze tymczasowym (np. zapisy na kolędę, zapisy na rekolekcje), podlega rygorom Dekretu KEP z 2018 r. Na administratorze spoczywa bezpośredni obowiązek wdrożenia standardów technicznych i organizacyjnych z art. 6 i 17 tego aktu normatywnego. Wyklucza to swobodę w doborze zabezpieczeń o zaniżonym standardzie. Po drugie, elektroniczne odpowiedniki ksiąg parafialnych muszą być traktowane jako integralna część systemu dokumentowego Kościoła. Nakłada to na podmioty kościelne obowiązek wdrożenia rozwiązań informatycznych, które zagwarantują zbiorom cyfrowym wiarygodność, autentyczność i rygor niezniszczalności na poziomie równym tradycyjnym księgom materialnym. Po trzecie, praktyka kancelaryjna powinna być interpretowana z naciskiem na *ratio legis* historycznych regulacji. Wykładnia funkcjonalna dawnych norm wymaga, aby rozstrzyganie ewentualnych kolizji między tradycyjnym prawem a cyfrową praktyką zawsze służyło zabezpieczeniu pewności obrotu prawnego, integralności zapisów sakramentalnych oraz najwyższemu dobru, jakim jest ochrona informacji o osobie.

3.2. Postulaty *de lege ferenda*

Osiągnięcie pełnej przejrzystości w cyfrowym przetwarzaniu danych (KEP 2018, art. 5 ust. 1 pkt 1) i jednolitości praktyki w podmiotach kościelnych wymaga ingerencji prawodawczej na poziomie ogólnopolskim. Zmiany powinny usunąć zdiagnozowaną lukę w kościelnym prawie administracyjnym i ujednolicić praktykę w diecezjach, zakonach i innych jednostkach organizacyjnych. W tym obszarze, z perspektywy naukowej można zaproponować następujące kierunki zmian *de lege ferenda*.

Po pierwsze, Konferencja Episkopatu Polski powinna wydać nowy dekret ogólny (ustawę kościelną), który uzupełni lub definitywnie zastąpi zdezaktualizowane technologicznie Przepisy z 1947 r. Po drugie,

nowy akt normatywny musi precyzyjnie określać status kanoniczny elektronicznych ksiąg w procesach kanonicznych, relację między rejestrami papierowymi a cyfrowymi oraz tryb legalnego generowania wypisów uwierzytelnionych podpisem kwalifikowanym lub inną metodą zapewniającą wiarygodne potwierdzenie autentyczności osoby wystawiającej dokument. Po trzecie, niezbędne jest ujednolicenie minimalnych wymagań technicznych przetwarzania cyfrowego dla diecezji w Polsce, w tym wytycznych dla szyfrowania baz danych, dopuszczalności korzystania z konkretnych modeli usług chmurowych oraz procedur reagowania na cyberincydenty. Po czwarte, należy wzmocnić diecezjalnych i zakonnych inspektorów ochrony danych w procesie zatwierdzania oprogramowania lub rozwiązań technicznych przeznaczonych dla podmiotów kościelnych. Po piąte, prawodawca powinien wprost uregulować obowiązek przeprowadzania oceny skutków dla ochrony danych dla scentralizowanych systemów metrykalnych i oświatowych jeszcze przed ich wdrożeniem produkcyjnym. Po szóste, nowe prawo musi wprost odpowiadać na unikalną specyfikę i ontologię kościelnych danych sakramentalnych (informacje o chrzcie, święceniach, karach kanonicznych). Po siódme, należy precyzyjnie skodyfikować w środowisku cyfrowym ograniczenia w stosowaniu „prawa do usunięcia danych” (KEP 2018, art. 13), zasady trwałości zapisów oraz rygory informatycznego oznaczania zmian statusu kanonicznego (np. z powodu kar kościelnych czy adnotacji o złożeniu oświadczenia woli o wystąpieniu z Kościoła).

Podsumowanie

Powszechne wykorzystywanie przez podmioty kościelne elektronicznych systemów przetwarzania danych obnaża istotną lukę prawną w systemie prawa kanonicznego. Nie dotyczy ona jednak samej ochrony danych osobowych – ta bowiem jest zabezpieczona Dekret KEP z 2018 r. Luka obejmuje brak norm kościelnego prawa administracyjnego, które określałyby rygory i formy prowadzenia ewidencji metrykalnej w przestrzeni cyfrowej. Próba uzupełnienia tej luki w drodze realizacji postulatów *de lege lata* stanowi rozwiązanie doraźne i niewystarczające. Z punktu widzenia zasady pewności

prawa oraz skutecznej ochrony danych sakramentalnych wiernych niezbędne jest zrealizowanie sformułowanych w artykule postulatów *de lege ferenda*.

Na kościelnych prawodawcach, a w szczególności Konferencji Episkopatu Polski oraz biskupach diecezjalnych czy wyższych przełożonych zakonnych, spoczywa obowiązek pogłębionej analizy wpływu cyfryzacji na funkcjonowanie Kościoła. Zmiana nośnika danych z ksiąg papierowych na systemy informatyczne wymaga od ustawodawcy ustanowienia odpowiednich norm prawnych. Na wskazanych prawodawcach zgodnie z art. 2 Dekretu KEP z 2018 r. spoczywa obowiązek pogłębionej analizy wpływu zmian technologicznych (od ksiąg papierowych do systemów informatycznych) na działanie Kościoła jako instytucji oraz na życie wspólnoty wiernych, a także oblige do nowego wypowiedzenia się co do podstaw i form, w jakich dane osobowe mogą być przetwarzane. Zgodnie z art. 37 ust. 1 pkt 9 Dekretu KEP z 2018 r., aktywną rolę w tym procesie powinien odegrać KIOD, który ma kompetencje do przedkładania Konferencji Episkopatu Polski propozycji nowych regulacji prawnych lub zmian w przepisach już obowiązujących.

Kościół w Polsce, mając zagwarantowaną autonomię regulacyjną w obszarze ochrony danych osobowych, powinien rzeczywiście tę autonomię wykonywać poprzez przepisy, które realizowałyby zasadę odpowiedzialności legislacyjnej wobec wspólnoty wiernych.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: Not applicable.

AI tools: Not applicable.

Conflicts of Interest: The author declares no competing interests.

References

Sources

- Archidiecezja Lubelska. 2018. *Przewodnik po nowych przepisach dotyczących ochrony danych osobowych dla osób pełniących posługę w Kościele katolickim na terytorium Polski (stan prawny na dzień 25 maja 2018 roku). Materiały pomocnicze przygotowane dla uczestników szkolenia w Archidiecezji Lubelskiej*. https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=http://pliki.diecezja.lublin.pl/ODO/ochrona_danych_osobowych_szkolenie.docx.pdf&ved=2ahUKEwixjr-n2_mUAXWmBtsEHRQePN4QFnoECBoQAQ&usg=AOvVaw3azQPKw0M6UhJBzmfkdLX. Accessed: 9 June 2026 (=AL.).
- Archidiecezja Wrocławska. 2018. Instrukcja dotycząca prowadzenia kartoteki parafialnej. L.dz. 1279/2018, 22 października 2018 (=AW).
- Codex Iuris Canonici auctoritate Ioannis Pauli PP. II promulgatus*, 25.01.1983. AAS 75/II (1983): V-XXX. 1-317. Translation: *Kodeks Prawa Kanonicznego. Komentarz*. 2023. 2nd ed., edited by Piotr Majer. Warszawa: Wolters Kluwer (=CIC/83).
- Codex Iuris Canonici Pii X Pontificis Maximi iussu digestus Benedicti Papae XV auctoritate promulgatus*, 27.05.1917. AAS 9/II (1917): 2-521 (=CIC/17).
- Konferencja Episkopatu Polski. 2018. Dekret ogólny w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Kościele katolickim. *Akta Konferencji Episkopatu Polski* 30: 31-54 (=KEP).
- Konferencja Episkopatu Polski. 1947. Przepisy o prowadzeniu ksiąg parafialnych ochrzczonych, bierzmowanych, małżeństw i zmarłych oraz księgi stanu dusz (5-7 września 1947). In Franciszek Bączkowicz, Józef Baron and Władysław Stawinoga. 1958. *Prawo kanoniczne. Podręcznik dla duchowieństwa*. Vol. 2, 597-615. Opole: Wydawnictwo Św. Krzyża (=KEP).
- Kościelny Inspektor Ochrony Danych. 2023. Okólnik z dnia 20 grudnia 2023 r. dotyczący przetwarzania danych osobowych w systemach informatycznych (=KIOD).
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (OJL 119, 4.5.2016: 1-88).
- Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. 2017 r. poz. 459, ze zm.).

Literature

- Karsten, Kinga. 2021. „Kilka uwag dotyczących zastosowania dekretu Konferencji Episkopatu Polski o ochronie danych osobowych z 2018 r. do spraw małżeńskich lub rodzinnych.” *Annales Canonici* 17 (1): 23-37. <https://doi.org/10.15633/acan.3923>.

- Karsten, Kinga. 2025. „O niezależności inspektora ochrony danych w podmiotach kościelnych.” *Prawo Kanoniczne* 68 (3): 5-21. <https://doi.org/10.21697/pk.2025.68.3.01>.
- Kroczek, Piotr. 2020. *Przetwarzanie danych osobowych przez podmioty Kościoła katolickiego w Polsce: transfer pomiędzy państwami*. Kraków: Wydawnictwo UNUM.
- Kroczek, Piotr, and Piotr Skonieczny. 2022. *Ochrona danych osobowych w Kościele katolickim. Komentarz do Dekretu ogólnego Konferencji Episkopatu Polski w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Kościele katolickim z 2018 roku*. In *Annales Canonici. Monographiae*, no. 9. Vol. 1/1-2, edited by Józef Krzywda. Kraków: Wydawnictwo Naukowe Uniwersytetu Papieskiego Jana Pawła II.
- Morawski, Lech. 2010. *Zasady wykładni prawa*. 2nd ed. Toruń: TNOiK Dom Organizatora.
- Pawluk, Tadeusz. 1985. *Prawo kanoniczne według Kodeksu Jana Pawła II*. Vol. 1. Olsztyn: Warmińskie Wydawnictwo Diecezjalne.
- Sobiecka, Małgorzata. 2025. „Wyzwania Kościoła katolickiego w Polsce w związku z ogólnym rozporządzeniem o ochronie danych osobowych.” In *Refleksje wokół prawa kanonicznego*, edited by Dobrochna Bach-Golecka i Katarzyna Myszonaz-Kostrzewa, 279-298. Warszawa: Instytut Wydawniczy EuroPrawo.
- Sztafrowski, Edward. 1985. *Podręcznik prawa kanonicznego*. Vol. 1. Warszawa: Akademia Teologii Katolickiej.

Abstrakt

Problem badawczy: Brak ogólnopolskiego kościelnego aktu prawnego regulującego cyfrowe przetwarzanie danych osobowych w Polsce, w szczególności elektronicznych ksiąg parafialnych, tworzy istotną lukę prawną.

Cel przeprowadzonych badań: Wykazanie, w jaki sposób normy uzupełnienia luki prawnej z kan. 19, w połączeniu aktami kanonicznego prawa partykularnego, praktyką Kościelnego Inspektora Ochrony Danych mogą służyć do tymczasowego wypełnienia tej luki i ochrony praw wiernych.

Metody: W opracowaniu zastosowano dogmatyczną i funkcjonalną analizę wydanych przez Konferencję Episkopatu Polski: Dekretu z 2018 roku, przepisów z 1947 roku oraz wybranych aktów diecezjalnych, rozumowanie przez analogię w oparciu o kanon 19, a także analizę *soft law* i praktyki.

Wyniki badań: Wyniki wskazują, że mimo braku ogólnopolskich regulacji dotyczących cyfrowego przetwarzania danych w Kościele katolickim w Polsce, istniejące normy prawa kanonicznego, także te dotyczące ochrony danych pozwalają – poprzez analogię – na stosowanie tradycyjnych zasad prowadzenia ksiąg parafialnych do systemów informatycznych.

Wnioski z przeprowadzonych badań: Pilnie wymagane jest wydanie ogólnopolskiego kościelnego aktu normatywnego, który aktualizowałby lub zastępował przepisy

z 1947 roku. Powinien on m.in. ustalać minimalne standardy techniczne, wzmacniać rolę inspektorów ochrony danych i przewidywać jako obowiązkową ocenę skutków dla ochrony danych.

Słowa kluczowe: ochrona danych osobowych, przetwarzanie elektroniczne, prawo kanoniczne, księgi parafialne, luka prawna

PROCESSING OF DATA IN DIGITAL FORM BY CHURCH ENTITIES – *DE LEGE LATA* AND *DE LEGE FERENDA* POSTULATES

Abstract

The problem addressed: The lack of a nationwide ecclesiastical legal framework regulating the digital processing of personal data in Poland, particularly concerning electronic parochial registers, creates a significant legal gap.

The aim of the research conducted: To demonstrate how the provisions intended to address the legal gap in can. 19 CIC, in conjunction with acts of particular canon law and the practice of the Church Data Protection Officer, can serve to temporarily fill this gap and protect the rights of the faithful.

Methods: This study employed a dogmatic and functional analysis of documents issued by the Polish Bishops' Conference, including the 2018 Decree, the 1947 regulations, and selected diocesan acts. It also utilized analogy-based reasoning grounded in can. 19 CIC, along with an analysis of „soft law” and established practices.

The results of the research: The results indicate that, despite the absence of nationwide regulations governing digital data processing within the Catholic Church in Poland, existing norms of canon law, including those concerning data protection, permit, through analogy, the application of traditional principles governing parochial record-keeping to IT systems.

The conclusions drawn from the research: There is an urgent need for a nationwide ecclesiastical regulation that would update or replace the 1947 provisions. Such a regulation should, among other things, establish minimum technical standards, strengthen the role of data protection officers, and mandate data protection impact assessments.

Keywords: personal data protection, electronic processing, canon law, parochial registers, legal gap

Translated by Alan Kretkowski