International Journal of Contemporary Sciences (IJCS)
Vol. 4, No. 6, 2026: 1767-1784

Nurturing Faith in the Digital Age: Digital Security, Christian Ethics, and Faith Formation in Cyberspace

Rocky Agustry Vernando Simamora
Christian University of Indonesia
Corresponding Author: Rocky Agustry Vernando Simamora
2506190011@ms.uki.ac.id

A R T I C L E I N F O

Keywords: Digital Security, Christian Ethics, Faith Formation, Christian Digital Habitus, Christian Religious Education

Received : 15 April
Revised : 20 May
Accepted: 27 June

©2026 Simamora: This is an open-access article distributed under the terms of the Creative Commons Atribusi 4.0 Internasional.

A B S T R A C T

Digital transformation has made cyberspace a formative environment that shapes attention, relationships, habits, and faith. This article analyzes technical, moral, relational, and spiritual threats in cyberspace, formulates Christian ethics as the basis of digital stewardship, and argues that digital security and digital wellness function as protective and formative practices in faith formation. Using qualitative library research and conceptual analysis, this study examines theological, pedagogical, cybersecurity, digital ethics, and digital wellness literature; as a conceptual study, it uses no empirical sample or observation timeline. The findings show that Christian Religious Education must move beyond technical caution and moral advice toward holistic faith formation. The article contributes a synthesis that forms Christian digital habitus through discernment, integrity, responsibility, and self-control

DOI: https://doi.org/10.55927/hwq1tq54
E-ISSN: 3047-4078
https://journalijcs.my.id/index.php/ijcs

INTRODUCTION

Digital transformation has reshaped human life in fundamental ways. Cyberspace no longer functions merely as a supplementary channel for communication or information exchange. It has become a formative environment in which people learn, work, build relationships, construct opinions, and express religious life. In this context, faith is no longer practiced only in physical spaces, but also within digital spaces that shape how people understand themselves, others, and truth. Bingaman (2023, p. 1) describes digitalization as an irreversible process because digital technology has become deeply embedded in modern human life. This condition requires Christian Religious Education to take the digital environment seriously as a space of formation, not merely as a tool or external medium.

Christian engagement with technology should not be framed by rejection or uncritical acceptance. Christian faith does not call believers to be anti-technology, but to use technology wisely through ethical awareness, digital literacy, and responsibility before God and others. Boiliu et al. (2025, pp. 219–220) argue that digital media is not only a communication instrument, but also a formative environment that influences spiritual identity, ethical behavior, and the practice of Christian Religious Education in the digital era. Therefore, the central issue is no longer whether believers should be present in digital spaces, but how they can inhabit these spaces faithfully, responsibly, and critically.

This question becomes urgent because digital spaces also produce serious threats. These threats appear in technical forms such as phishing, data theft, online fraud, and identity misuse. Yet their impact goes beyond technical vulnerability. Digital threats damage trust, distort relationships, weaken moral responsibility, and affect the quality of Christian witness. Cyberspace is therefore not only a technological risk environment, but also a moral, relational, and spiritual field. When digital interaction becomes careless, manipulative, or violent, the problem is not limited to devices and systems. It reaches the human person, the community, and the formation of faith.

Existing discussions often treat digital security and Christian digital ethics as separate concerns. Digital security is commonly reduced to technical protection, risk awareness, and preventive procedures. At the same time, Christian digital ethics often remains at the level of general moral advice without sufficient attention to the formative power of digital platforms, algorithmic culture, emotional reactivity, and mediated relationships. Both approaches are necessary, but they are not sufficient. A purely technical approach cannot explain how hatred, misinformation, addiction, and digital impulsiveness shape character and weaken Christian witness. A purely moralistic approach cannot adequately address the structural and cultural logic of digital communication. This article therefore argues that digital security, Christian ethics, and digital wellness must be read together as a matter of faith formation.

The contribution of this article lies in its attempt to synthesize digital security, Christian ethics, and digital wellness within the framework of Christian Religious Education. Christian ethics provides the normative ground for digital stewardship. Digital security functions as a protective praxis that safeguards

data, identity, trust, and community life. Digital wellness functions as a formative praxis that orders attention, rhythm, emotion, and embodied presence in the midst of digital pressure. These three dimensions converge toward faith formation and the cultivation of Christian digital habitus. In this sense, the article does not merely ask how Christians can avoid digital threats. It asks how believers can be formed to live wisely, truthfully, and responsibly in cyberspace.

Based on this problem, this article asks how cyberspace generates technical, moral, relational, and spiritual threats; how Christian ethics can ground digital stewardship in the use of digital media; and how digital security and digital wellness can function as formative practices within Christian Religious Education. The focus is not only technical caution, but holistic faith formation in cyberspace, so that Christian presence in the digital age may be marked by discernment, relational integrity, digital responsibility, and self-control.

LITERATURE REVIEW

1. Digital Technology as a Cultural and Formative Space

Digital technology should be read as part of human culture, not merely as a technical instrument or external threat. In Christian Religious Education, human beings are cultural agents who think, create, communicate, and organize common life. From this perspective, digital technology expresses the human capacity to engage and shape social reality. This starting point prevents a technophobic view of cyberspace. Gulo and Tapilaha (2024, pp. 105–106) argue that Christian Religious Education in the digital era cannot simply preserve older pedagogical models because technological change has reshaped how people access information, communicate, and understand the world. Tarihoran et al. (2024, pp. 16–17) also show that technology can expand the possibilities of faith formation through interactive media, online resources, and learning spaces that are closer to digital generations, as long as its use remains careful and pedagogically responsible.

Yet the cultural location of digital technology does not make it neutral. Technology carries an ambivalent character because it stands within human creativity and human moral fragility at the same time. It can open new possibilities for learning, ministry, and faith formation, but it can also intensify distraction, manipulation, and dehumanization. Waruwu and Lawalata (2024, pp. 22–24) emphasize that digital technology 5.0 creates a complex environment in which Christian values such as honesty, justice, love, and responsibility must be integrated into digital culture. Immanuela (2024, pp. 81–82) notes that churches in the digital era face moral shifts, relativism, value conflicts, and social media pressures that may weaken faith integrity without serious education and accompaniment. Leone (2024, pp. 1–2) further argues that every technological leap carries forms of sacrifice, including the possible loss of depth, boundaries, and human wholeness when progress lacks ethical direction. Therefore, digital technology must be critically embraced. It is neither an enemy to reject nor a neutral tool to use without moral discernment.

2. Christian Ethics and Digital Stewardship

Christian ethics provides the normative basis for digital stewardship because digital life involves more than access, speed, and technical skill. It involves truth, identity, relationships, attention, emotion, and responsibility. Digital stewardship, therefore, cannot be reduced to safe media use. It refers to the faithful management of digital presence before God and others. Elizabeth and Mikaere (2025, pp. 55–56) show that the ethical challenge of the digital world is not located only in technology itself, but also in threats to accountability and spiritual integrity in Christian service. Digital engagement therefore cannot be separated from love, humility, justice, and stewardship. In a more pedagogical frame, Sari and Bermuli (2021, pp. 46–47) argue that technological development does not automatically produce moral development. Christian ethics must function as a foundation for character formation grounded in God's truth rather than in the relativism that often shapes digital culture.

Within this framework, Christian digital stewardship can be organized around three ethical principles. The first is truth and integrity. Digital communication requires verification, honesty, and responsibility because speed and virality often weaken the discipline of truth. The second is love, respect, and digital empathy. Digital interaction must recognize the dignity of persons behind accounts, comments, images, and messages, so disagreement does not become humiliation or dehumanization. The third is stewardship of speech, attention, and emotion. Digital platforms often intensify impulsive reactions, anger, and performative communication. Christian ethics therefore calls believers to govern not only what they say online, but also how they attend, respond, and participate. In this sense, digital ethics is not a list of prohibitions. It is a formative framework for cultivating Christian character in cyberspace.

3. Faith Formation, Shared Praxis, and Christian Digital Habitus

Thomas H. Groome's concept of shared praxis helps explain why digital experience must enter the field of faith formation. Groome (1991, p. 18) argues that the purpose of Christian education is to form faith that is truly lived. Religious education therefore should not stop at the transmission of knowledge. It must inform, form, and transform persons within the lived reality of Christian faith. The strength of shared praxis lies in its movement from concrete life experience to critical reflection, from reflection to engagement with the Christian story and vision, and from that engagement to responsible decision and action (Nagle, 2019, pp. 2, 4–6). This approach matters in the digital era because digital experience is not external to faith. It shapes attention, relationships, moral judgment, and religious imagination. For this reason, digital experience must be brought into theological reflection rather than being left to operate silently as an unexamined teacher.

James K. A. Smith (2009, pp. 27, 29) deepens this argument by showing that human beings are shaped not only by what they think, but by what they love. Education is never neutral because every formative practice directs desire, shapes imagination, and trains a particular vision of the good life. Smith (2009, p. 55) also argues that repeated practices can form habitus, or a second nature, which later works almost spontaneously in human life. In the digital context,

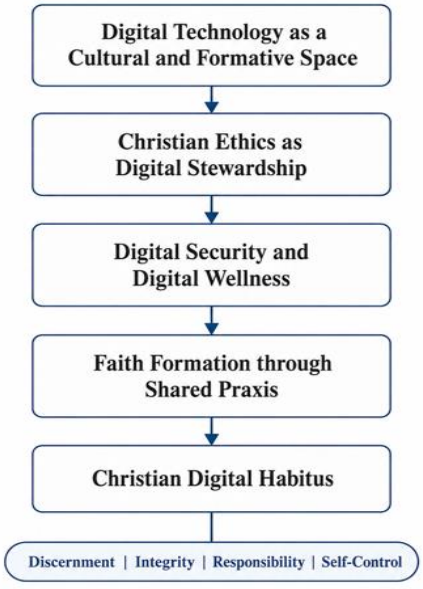
social media, notifications, viral culture, and short-form video streams are not merely channels of communication. They are cultural practices that train attention, stimulate desire, accelerate response, and gradually shape disposition. The digital problem is therefore not only the presence of harmful content. It is also the kind of person being formed through daily digital habits.

This article uses the term Christian digital habitus to describe a relatively stable disposition formed through faith within digital life. Oliver et al. (2020, p. 130) refer to a spiritually wise digital habitus as the capacity to apply wisdom from spiritual traditions to socially mediated digital participation. This insight shows that Christian presence online cannot be measured merely by the frequency of religious posts, but by the wisdom that shapes interaction, response, boundaries, and attention. La Cruz and Mora (2024, pp. 3–4) also describe digital habitus as an internalized system of schemes that generates thoughts, actions, desires, and perceptions within digital culture. Thus, Christian digital habitus is not a decorative religious identity in cyberspace. It is the fruit of faith formation that shapes how believers discern, communicate, protect others, and govern themselves in digital environments.

4. Conceptual Framework

This article develops a conceptual framework for reading digital life as a cultural and formative space marked by concrete threats to truth, trust, identity, and community. Within this framework, Christian ethics functions as the normative ground of digital stewardship. Digital security functions as protective praxis that safeguards data, identity, trust, and community life from external threats. Digital wellness functions as formative praxis that orders attention, emotion, rhythm, and presence from within. Faith formation integrates these practices through theological reflection and responsible action. The expected outcome is Christian digital habitus, expressed through discernment, relational integrity, digital responsibility, and self-control.

Figure 1. Conceptual Framework of Christian Digital Habitus Formation



METHODOLOGY

This article employed a qualitative conceptual design through library research and conceptual analysis. It did not seek to measure variables, test hypotheses, or generalize from empirical respondents. Its purpose was to construct an integrated conceptual framework for interpreting digital security, Christian ethics, digital wellness, and faith formation in cyberspace. The textual materials analyzed in this study consisted of selected theological, pedagogical, digital ethics, cybersecurity, and digital wellness literature, including scholarly books, peer-reviewed journal articles, and relevant institutional reports. Since this is a conceptual study, it did not involve field participants, empirical samples, or observation timelines. The literature was selected based on its relevance to four conceptual domains: digital threats, Christian digital stewardship, faith formation, and Christian digital habitus.

The analytical procedure followed a systematic process of conceptual reading and synthesis. First, the literature was selected and focused according to the research questions. Second, key arguments were condensed into thematic categories, including cyberspace threats, digital stewardship, protective praxis, formative praxis, and faith formation. Third, these categories were organized into a conceptual display to clarify their relationships. Fourth, the emerging synthesis was examined for conceptual coherence, theological relevance, and pedagogical implications. This procedure follows the account of qualitative analysis proposed by Miles et al. (2014, pp. 8–10), which describes analysis as an interactive process of data condensation, data display, and conclusion drawing or verification. It also follows the view of Ravitch and Riggan (2017, pp. 26, 30) that a conceptual framework is an argument about why a topic matters and why the theoretical and methodological choices used to study it are appropriate and rigorous. Through this process, the article develops a framework in which Christian ethics provides the normative ground, digital security functions as protective praxis, digital wellness functions as formative praxis, and faith formation leads toward Christian digital habitus.

RESULTS AND DISCUSSION

1. Cyberspace Threats

Cyberspace must be examined as a field of risk because digital threats no longer attack only devices, systems, or platforms. They also enter the domains of truth, relationships, trust, and Christian witness. One of the most visible threats is misinformation and disinformation. In Indonesia, the Ministry of Communication and Digital Affairs (2025) identified and clarified 1,923 pieces of hoax-related content throughout 2024, with the highest number recorded in October at 215 cases. Fraud-related hoaxes became the dominant category. This figure shows that the Indonesian digital sphere is not only dense with information but also filled with manipulative content that distorts public discernment and weakens the ability to distinguish truth from deception.

This danger becomes more complex when misinformation appears not only in written form, but also through video, audio, and images that are easier to trust. Juditha and Darmawan (2024, p. 167) note that in early 2024, the Indonesian government had handled 2,882 pieces of hoax-related content on social media,

203 of which were related to the 2024 election. They also show that manipulated hoaxes were widely circulated through YouTube and TikTok, while artificial intelligence-based hoaxes were becoming increasingly prominent. A 2026 report from the Yogyakarta Center for Human Resources Development and Research in Communication and Digital Affairs (BPSDMP Komdigi Yogyakarta) further indicates that deepfake attacks increased by 1,400 percent year-on-year from 2024 to 2025, while AI-based phishing also rose sharply, with a reported success rate of 54 to 60 percent (Kementerian Komunikasi dan Digital, 2026). These developments indicate that digital threats are no longer limited to ordinary false information. They now include the manipulation of faces, voices, images, and identities that can deceive both verification systems and human perception. For Christian communities, this condition is highly consequential. Sermon clips, theological statements, or public remarks from church leaders can be edited, removed from context, or fabricated in ways that damage reputation, create suspicion, and weaken communal trust.

Cyberspace also threatens human dignity through cyberbullying and hate speech. WHO Europe (2024) reported that one in six school-aged children experienced cyberbullying. UNICEF (2019) also reported that one in three young people in 30 countries had experienced online bullying, and one in five had skipped school because of it. These data show that digital space is not merely a site of interaction. It can also become a space where social and psychological wounds are produced and intensified. In Indonesia, this problem is also evident. Muannas and Mansyur (2020, p. 125) argue that Indonesia has a very high level of social media use, but weak digital literacy often causes users to lose control and participate in hate speech. From a Christian perspective, cyberbullying and hate speech cannot be treated merely as inappropriate online behavior. They violate human dignity and show how digital environments can form reactive, aggressive, and empathy-poor characters when they are not critically guided.

Another serious set of threats involves phishing, online fraud, and impersonation. These threats work by exploiting something deeply human: trust. The Anti-Phishing Working Group (2025, p. 2) reported 1,003,924 phishing attacks in the first quarter of 2025, indicating the massive scale of this threat. In Indonesia, ANTARA cited the Ministry of Communication and Informatics as stating that from 2017 to 2024, the *cekrekening.id* service received 572,000 reports of bank accounts linked to online fraud. Online buying and selling fraud dominated the reports, with 528,415 complaints, followed by 43,770 complaints related to fictitious investment schemes (Rochman, 2024). The destructive power of digital threats was also visible in the 2024 ransomware attack on Indonesia's National Data Center. Reuters (2024) reported that the attack affected more than 160 government agencies and involved an 8 million US dollar ransom demand, while 98 percent of the data in one affected data center reportedly had no adequate backup. If digital threats can paralyze public services and erode trust at the state level, similar threats cannot be treated lightly at the level of churches, schools, and Christian communities.

These cases show that cyberspace is not only a space of information exchange. It is also a space where trust, innocence, solidarity, and institutional

credibility can be exploited. In Christian communities, this risk becomes more serious when perpetrators misuse the names of pastors, church leaders, ministry committees, school administrators, or trusted members to obtain money, personal data, or digital access. In such cases, digital threats do not merely attack individual users. They attack the network of trust that sustains ecclesial, educational, and familial life. Therefore, digital security is not only a technical concern. It is also a communal and moral responsibility.

Based on this analysis, cyberspace threats operate at three interconnected levels. First, they threaten data and privacy. When congregational data, pastoral communication, ministry documents, or family identities are leaked or misused, the damage affects not only administrative systems but also the dignity and sense of safety of the community. Second, they threaten relationships and trust. Cyberbullying, online fraud, impersonation, and hate speech create suspicion, emotional wounds, and relational fractures. Third, they threaten narrative and doctrine. Hoaxes, manipulated sermon clips, and deepfakes weaken the community's ability to distinguish truth from manipulation and may be used to divide believers. These threats show that the central question is not simply whether Christians should use digital technology, but whether they can inhabit digital space without losing truth, love, integrity, and faithfulness. Without theological, ethical, and pedagogical discernment, cyberspace can shift from a space of learning and ministry into a space that fragments attention, fractures community, and damages Christian witness.

2. Christian Ethical Responses to Digital Threats

Cyberspace threats require more than technical caution. They demand a Christian ethical response to distorted truth, manipulated identity, violated dignity, and unmanaged emotion. In this section, Christian ethics is not treated as general moral advice, but as a concrete response to the ways digital environments deform communication, weaken trust, and normalize careless participation. Three responses are decisive: truth and integrity, love and digital empathy, and the stewardship of speech, attention, and emotion.

Truth and integrity form the first response because misinformation, deepfake manipulation, and decontextualized content damage the moral conditions of communal life. Digital media works through speed, repetition, and engagement. Under this logic, the fastest information often appears more persuasive than the most accurate information. Caled and Silva (2022, pp. 123–124) show that digital media enables users to produce and circulate unverified content, while the source and context of an upload often become difficult to trace. Verification, therefore, is not a minor technical habit. It is a moral responsibility. Ephesians 4:25 gives a theological ground for this responsibility by placing truth-telling inside the life of the community. To speak truth in digital space means refusing to share unverified information, refusing to distort quotations, and refusing to circulate sermon clips, public statements, or theological claims outside their proper context.

Integrity also concerns identity. Digital culture rewards visibility, influence, and performance. This can encourage users to curate an image that is

more strategic than truthful. The ethical problem becomes sharper when identity is used to deceive, impersonate, manipulate authority, or build false credibility. Such acts do not merely violate digital etiquette. They damage Christian witness. Kia and Majesty (2026, p. 83) emphasize that Christian digital communication requires truthful speech and wise participation, so cyberspace can become a channel for responsible witness rather than a threat to it. Integrity, therefore, demands transparent identity, accurate context, and the willingness to correct mistakes. A Christian digital presence cannot separate visibility from truthfulness.

Love, respect, and digital empathy form the second response. Cyberbullying and hate speech expose how easily digital interaction can erase the person behind the account. Bularca et al. (2024, p. 1) show that cyberbullying on social media includes verbal harassment, threats, humiliation through sensitive content, exclusion from groups, and the exposure of personal secrets, while many bystanders remain silent. This means digital violence is sustained not only by aggressors, but also by passive spectators. Matthew 22:39 grounds the Christian response: the neighbor must be loved as oneself. In cyberspace, this command means that a person must never be reduced to a target of ridicule, humiliation, or exclusion. Anti-cyberbullying is therefore not merely a demand for polite communication. It is a defense of human dignity.

This ethical demand also applies to hate speech. Anttila and Domínguez-Armas (2025, pp. 695–696) argue that hate speech can operate as argumentative exclusion, which removes persons or groups from fair participation in public discourse. This insight sharpens the issue. The deepest problem with hate speech is not only its harsh language, but its attempt to deny others recognition as moral subjects. Christian ethics does not abolish correction, disagreement, or public critique. It rejects speech that humiliates, dehumanizes, and silences. Love in digital space is not mere tolerance. It is a disciplined regard for the dignity of the other.

The third response concerns the stewardship of speech, attention, and emotion. Digital conflict often begins not with planned malice, but with unmanaged reaction. Steinert and Dennis (2022, pp. 1–2) explain that social media contains emotional affordances, namely features that enable, encourage, and amplify emotional responses through notifications, instant feedback, and repeated interaction. These affordances help explain why digital spaces can quickly become arenas of anger, retaliation, and impulsive judgment. James 1:19 offers a counter-rhythm: quick to listen, slow to speak, and slow to anger. This is not a call to silence. It is a moral correction to a digital culture that treats speed as virtue and reaction as relevance.

For Christian Religious Education, these ethical responses must not remain external rules. Faith education does not stop at the transmission of doctrine. It forms ways of thinking, speaking, responding, and relating. Truth trains verification. Integrity trains honest presence. Love trains recognition of dignity. Stewardship of speech and emotion trains restraint. Without these practices, digital space will continue to form users who are reactive, easily provoked, and careless with the truth. With these practices, cyberspace can

become an arena where Christian faith is practiced with maturity, clarity, and responsibility. Christian ethics thus turns digital discernment into a concrete practice of truthful, dignified, and responsible participation.

3. Digital Security and Digital Wellness as Protective-Formative Praxis

Christian ethics remains incomplete if it does not become practice. In Christian Religious Education, digital formation cannot stop at knowing what is dangerous or what is morally right. It must train believers to live safely, wisely, and responsibly within digital environments. Digital security and digital wellness serve this task through two related movements. Digital security protects persons and communities from external threats such as fraud, data leakage, identity abuse, and unauthorized access. Digital wellness forms internal habits that order attention, emotion, rhythm, and presence. Together, they prevent digital education from remaining at the level of moral instruction and move it toward lived practice. This direction is consistent with the need to connect technology with spiritual formation, biblical community, responsible habits, self-control, and wisdom in Christian education (Chrismastianto et al., 2022, pp. 255–256; Sipahutar et al., 2025, pp. 800–801).

Digital security should first be read as protective praxis. It includes technical procedures such as two-factor authentication, password management, data backup, and access control. These tools matter, but they remain instruments. They cannot carry the whole moral weight of digital life. When security is reduced to devices, software, or procedural compliance, it fails to address the habits that make a community vulnerable. Salam et al. (2026, pp. 1–3, 11) show that cyber vulnerability in digitalized institutions grows not only from system weaknesses, but also from low awareness, limited training, and weak integrated policy. This finding matters for churches, schools, and Christian communities. Digital security fails when responsibility is not trained as a communal habit.

Digital security must therefore become a culture of communal vigilance. A donation request sent under the name of a pastor, treasurer, committee chair, or ministry leader should not be trusted merely because the sender looks familiar. It needs secondary verification through another channel. Congregational data, catechism class records, phone numbers, aid recipient lists, ministry documents, and pastoral conversations should not be shared widely simply because a digital group is considered internal. A screenshot of a private conversation is not a small matter when it exposes confidentiality, damages trust, or violates pastoral care. In such cases, digital failure becomes relational failure. Safety weakens, trust erodes, and the community learns that digital closeness does not automatically mean protection.

For this reason, digital security becomes a practical expression of Christian love. It protects others from negligence, prevents communities from manipulation, and refuses naïveté that is often mistaken for trust. This does not mean cultivating suspicion toward every digital interaction. It means cultivating disciplined care for data, identity, privacy, and relational trust. A Christian community that practices digital security learns to verify before acting, limit access before data is misused, protect confidential communication before

relationships are damaged, and treat digital responsibility as part of love for neighbor. Security becomes protective praxis when it guards the fragile conditions that make communal life possible.

Yet a safe digital life is not complete when a person is merely protected from fraud or data misuse. A believer may avoid phishing and still become distracted, exhausted, reactive, and unable to remain present. This is where digital wellness becomes formative praxis. Laffier et al. (2025, pp. 1–2) define digital wellness as the development of a healthy relationship with technology so that people can flourish and relate well in digital environments. They connect digital wellness with self-awareness, mindfulness, self-regulation, and conflict management. The issue is not simply how many hours a person uses a phone. The deeper question is whether digital life still allows a person to be present in learning, prayer, worship, work, family, and community.

Digital wellness gives moral and pedagogical weight to boundaries. Boundaries are not punishment against technology. They are practices of self-governance. Fu and Sideris (2024, pp. 469–470, 482) show that digital disconnection does not always mean withdrawing completely from digital life. It can take the form of limiting certain applications, avoiding features that intensify attachment, or creating pauses that allow affective and social recovery. Arness and Ollis (2023, pp. 24379–24380) further show that problematic social media use relates to attention dysregulation, including difficulty controlling the urge to reopen social media, seek validation, or shift attention impulsively. These findings clarify why digital wellness cannot be taught as a shallow instruction to "use the phone less." It requires practices that train attention, restraint, and presence.

In Christian practice, such formation can take concrete forms: turning off nonessential notifications, setting boundaries for digital communication, creating tech-free spaces at the dining table or during worship, and keeping time for silence without devices. These actions may look ordinary, but they form the capacity to be fully present before God, others, and oneself. The idea of a digital Sabbath belongs here. It is not a rejection of technology. It is a spiritual practice of stopping, creating distance, and refusing constant availability to the digital stream. Kia and Majesty (2026, pp. 84–85) frame this kind of digital pause as a way of recovering presence and spiritual orientation in digital life. Digital wellness becomes formative praxis because it trains believers not to be governed by notification, urgency, validation, or emotional impulse.

Digital security and digital wellness must therefore be held together. Digital security protects the community from external threats such as fraud, data leakage, and identity misuse. Digital wellness addresses internal disorders such as fragmented attention, exhaustion, dependency, and the loss of healthy boundaries. If digital security fails, the community becomes vulnerable to attack. If digital wellness fails, the person becomes governed by digital demands. A community that stresses security alone may become cautious but still exhausted and reactive. A community that stresses wellness alone may feel balanced, but remain careless with data and trust. In Christian Religious Education, both are practices of faith. Digital security trains responsibility and protection of others.

Digital wellness trains self-control, healthy boundaries, and full presence. Together, they form a digital life that is safe, responsible, and spiritually ordered.

4. Toward a Christian Digital Habitus

Digital security, Christian ethics, and digital wellness converge in one pedagogical direction: the formation of a Christian digital habitus. This habitus does not refer to religious activity online in a superficial sense. It names the settled pattern by which faith shapes perception, judgment, speech, responsibility, and restraint in digital environments. The need for such a habitus becomes clear because digital media have become lived spaces that shape consciousness, values, identity, spirituality, and social relations, not merely channels of communication (Dwiraharjo & Putrawan, 2026, pp. 1–2). For Christian Religious Education, the issue is therefore not only what believers access online, but how repeated digital practices form the kind of persons they become. This is where faith formation must bridge confessed belief and lived reality through identity clarification, reflection, and an integrated Christian way of life (Moyo & Pali, 2025, pp. 1–2).

A Christian digital habitus grows when digital discipleship moves beyond content delivery. Darmawan et al. (2024, pp. 1, 4) show that digital discipleship can support youth faith growth when it is connected with mentoring, spiritual life, service, and mission. This point matters for the argument of this article. Christian formation in cyberspace cannot rely on religious posts, online worship clips, or moral warnings alone. It requires practices that train believers to judge what is true, speak with integrity, protect others, govern attention, and resist digital pressures that reward speed, visibility, and reaction. Habitus is formed when these practices become stable patterns of response, not occasional acts of caution.

The first marks of this habitus are discernment and integrity. Discernment resists the speed of digital circulation. It trains believers to examine information, delay reaction, test truth, and refuse manipulated content. This matters because algorithmic environments do not simply display religious communication. They filter, amplify, and rank it. Fahed (2025, p. 12) shows that algorithms function as gatekeepers of religious presence and shape what is heard, ignored, and valued in digital religious life. Christian discernment therefore asks more than whether content sounds religious. It asks whether it is true, contextual, charitable, and responsible. Integrity strengthens this discernment. It refuses false identity, spiritual performance, decontextualized teaching, and witness that seeks visibility without truthfulness. Christian presence in cyberspace loses moral weight when it becomes image management.

The second marks are responsibility and self-control. Responsibility means that digital action carries moral consequences. A forwarded message, screenshot, edited video, exposed file, public comment, or financial request can protect a community or injure it. In this sense, responsibility gathers the ethical and protective dimensions discussed earlier: guarding data, protecting pastoral communication, verifying requests, and refusing to circulate private material without consent. Self-control addresses the inner side of the same formation. It

trains believers to set boundaries, govern attention, manage emotion, practice digital pauses, and refuse domination by notifications, urgency, and validation. Dwiraharjo and Putrawan (2026, p. 7) argue that digital spirituality must be relationally and ethically demanding, oriented toward empathy, dialogue, and communal responsibility rather than uncritical adaptation to consumerist logic. Lontoh and Wibowo (2025, pp. 1, 12) also show that digital worship and virtual community create new possibilities for engagement, yet raise serious questions about authenticity, intimacy, and spiritual depth. These concerns confirm that Christian digital habitus must form both outward responsibility and inward discipline.

The conceptual contribution lies here. Digital security protects the vulnerable conditions of communal life. Christian ethics gives normative direction to truth, dignity, and responsibility. Digital wellness orders attention, emotion, rhythm, and presence. None of these elements is sufficient in isolation. Together, they become pedagogical pathways toward a Christian digital habitus marked by discernment, integrity, responsibility, and self-control. Churches and Christian educational institutions, therefore, cannot be satisfied with digital activity, online reach, or religious visibility. They must become formative communities within digital culture. Digital transformation already touches worship, pastoral care, education, and community development (Schlag et al., 2025, pp. 1–2). The task of Christian Religious Education is to form believers who can inhabit cyberspace with faithfulness, truthfulness, care, and disciplined freedom. A Christian digital habitus is faith made durable in the habits of digital life.

CONCLUSIONS AND RECOMMENDATIONS

Cyberspace must be treated as a formative environment that shapes attention, relationships, habits, trust, and Christian witness. Digital threats affect more than devices and systems. They damage data and privacy, relationships and trust, narrative and doctrine, as well as the quality of Christian presence in public digital life. For this reason, Christian Religious Education cannot respond to digital culture only through technical caution or general moral advice. It requires an integrated pedagogical response in which Christian ethics gives normative direction, digital security protects communal life, and digital wellness forms healthy patterns of attention, emotion, rhythm, and presence.

The main contribution of this article is the synthesis of digital security, Christian ethics, and digital wellness as pedagogical pathways toward a Christian digital habitus. This habitus is expressed through discernment, integrity, responsibility, and self-control. Discernment trains believers to test information and resist manipulation. Integrity forms truthful digital presence. Responsibility protects data, trust, and community life. Self-control orders digital boundaries and prevents believers from being governed by notification, urgency, and online validation. Faith formation in the digital age therefore moves beyond knowing what is right. It trains believers to live rightly, wisely, and responsibly in cyberspace.

The implementation of this argument requires concrete practices in churches, families, schools, and Christian educational institutions. Churches

need protocols for protecting congregational data, verifying financial requests, managing digital communication, and guarding pastoral confidentiality. Schools and Christian education programs need to integrate digital security, ethical communication, digital wellness, and theological reflection into learning activities. Families need to cultivate shared digital rhythms, responsible media use, tech-free spaces, and regular conversations about faith and digital life. These practices should not aim at withdrawal from digital culture. They should form believers who can inhabit digital spaces with truthfulness, care, critical discernment, and faithful witness.

ADVANCED RESEARCH

This study is limited to conceptual and literature-based analysis. It does not use empirical fieldwork, interviews, surveys, classroom observation, or congregational case studies. Its proposed framework therefore still needs to be tested in concrete educational, ecclesial, and family contexts. Future research may examine how Christian digital habitus is formed among learners, families, educators, pastors, and church communities through empirical qualitative or mixed-method studies.

Further studies may also evaluate the practical use of digital security and digital wellness programs in Christian Religious Education. Research can examine how churches protect pastoral data, how schools teach ethical digital communication, how families practice digital Sabbath, and how youth groups build habits of discernment, integrity, responsibility, and self-control. Comparative studies across denominations, age groups, urban and rural contexts, and hybrid worship communities would help refine the framework. Such research can test, strengthen, or revise the conceptual model proposed in this article.

REFERENCES

Anti-Phishing Working Group. (2025). *Phishing Activity Trends Report, 1st Quarter 2025*. https://docs.apwg.org/reports/apwg_trends_report_q1_2025.pdf

Anttila, S., & Domínguez-Armas, Á. (2025). Argumentative Exclusion and the Case of Online Hate Speech. *Topoi*, *44*(3), 695–705. https://doi.org/10.1007/s11245-025-10165-9

Arness, D. C., & Ollis, T. (2023). A mixed-methods study of problematic social media use, attention dysregulation, and social media use motives. *Current Psychology*, *42*, 24379–24398. https://doi.org/10.1007/s12144-022-03472-6

Bingaman, K. A. (2023). Religion in the Digital Age : An Irreversible Process. *Religions*, *14*(108), 1–14. https://doi.org/10.3390/rel14010108

Boiliu, E. R., Jura, D., & de Carvalho, A. O. (2025). Reinterpreting Religion in the Digital Age: Theology, Ethics, and Christian Education. *Didache: Journal of Christian Education*, *6*(2), 219–242. https://doi.org/10.46445/djce.v6i2.1075

Bularca, M. C., Cristescu, S., & Netedu, A. (2024). Analyzing the cyberbullying phenomenon on social media from the perspective of students. *Frontiers in Psychology*, *15*(1458079), 1–15. https://doi.org/10.3389/fpsyg.2024.1458079

Caled, D., & Silva, M. J. (2022). Digital media and misinformation: An outlook on multidisciplinary strategies against manipulation. *Journal of Computational Social Science*, *5*(1), 123–159. https://doi.org/10.1007/s42001-021-00118-8

Chrismastianto, I. A. W., Wibawanta, B., Mumu, B., Sitepu, D. S., & Milenia, M. (2022). Teacher's Competencies Profile in Digital Technology Era: Spiritual Formation and Biblical Community. *POLYGOT: Jurnal Ilmiah*, *18*(2), 255–268. https://doi.org/10.19166/pji.v18i2.5742

Darmawan, I. P. A., Tanhidy, J., & Doma, Y. (2024). Youth key persons' digital discipleship process during the pandemic and post-pandemic era. *HTS*, *80*(1), 1–9. https://doi.org/10.4102/hts.v80i1.9673

Dwiraharjo, S., & Putrawan, B. K. (2026). From sacred space to cyberspace: Digital spirituality and millennial social relations. *Verbum et Ecclesia*, *47*(1), 1–8. https://doi.org/10.4102/ve.v47i1.3761

Elizabeth, E., & Mikaere, G. (2025). Christian Service Ethics in Facing the Challenges of the Digital World: A Theological-Ethical Perspective on Digital Engagement. *Ministries and Theology*, *02*(02), 55–64. https://doi.org/10.35335/2jna6x92

Fahed, Z. (2025). Digital Shepherds in Lebanon: Christian Witness, Sacred Algorithms, and Theological Mission in a Surveilled Age. *Religions*, *16*(1506), 1–16. https://doi.org/10.3390/rel16121506

Fu, J., & Sideris, M. (2024). Digital Disconnection of Australian Young Adults During the COVID - 19 Pandemic — Practices and Enablers. *Journal of Applied Youth Studies*, *7*(4), 469–486. https://doi.org/10.1007/s43151-024-00140-3

Groome, T. (1991). *Sharing Faith: A Comprehensive Approach to Religious Education and Pastoral Ministry. The Way of Shared Praxis*. Wipf and Stock Publishers.

Gulo, R. P., & Tapilaha, S. R. (2024). Reforming Christian Religious Education: Integrating Spirituality and Critical Reasoning in the Digital Era. *Didache: Journal of Christian Education*, *5*(2), 105–123. https://doi.org/10.46445/djce.v5i2.823

Immanuela. (2024). The Role of the Church in Maintaining the Integrity of Faith Amidst Changing Morality in the Digital Era. *International Journal of Christian Education and Philosophical Inquiry*, *1*(4), 81–90.

https://doi.org/10.61132/ijcep.v1i4.83

Juditha, C., & Darmawan, J. J. (2024). Komunikasi Politik Terkait Hoaks Pada Pemilu Presiden Indonesia 2024. *Jurnal Studi Komunikasi Dan Media*, *28*(2), 167–182. https://doi.org/10.17933/jskm.2024.5682

Kementerian Komunikasi dan Digital. (2025). *Komdigi Identifikasi 1.923 Konten Hoaks Sepanjang Tahun 2024*. Kementerian Komunikasi Dan Digital. https://www.komdigi.go.id/berita/siaran-pers/detail/komdigi-identifikasi-1923-konten-hoaks-sepanjang-tahun-2024

Kementerian Komunikasi dan Digital. (2026). *AI Jadi Senjata Siber, Deepfake Naik 1.400 Persen - Wamen Komdigi Buka Workshop Cybersecurity #13 di Yogyakarta*. BPSDMP Komdigi Yogyakarta. https://bpsdm.komdigi.go.id/upt/yogyakarta/berita-ai-jadi-senjata-siber-deepfake-naik-1-400-persen-wamen-komdigi-buka-worksho-5-88

Kia, A. D., & Majesty, G. T. (2026). Keamanan Digital dan Etika Kristen di Ruang Maya. In *Pendidikan Kristen dan Teknologi Digital* (pp. 79–86). Widina Media Utama.

La Cruz, A., & Mora, F. (2024). Researching Artificial Intelligence Applications in Evangelical and Pentecostal/Charismatic Churches: Purity, Bible, and Mission as Driving Forces. *Religions*, *15*(234), 1–14. https://doi.org/10.3390/rel15020234

Laffier, J., Rehman, A., & Westley, M. (2025). The Promise of Digital Wellness to Promote Youth Well-Being and Healthy Communities. In J. Ferreira (Ed.), *Interpersonal Relationships in the Contemporary 21st Century Society* (pp. 1–23). https://doi.org/10.5772/intechopen.1008817

Leone, M. (2024). Technology and Sacrifice. *Religions*, *15*(692), 1–17. https://doi.org/10.3390/rel15060692

Lontoh, F. O. L., & Wibowo, D. A. (2025). Digital Pentecostalism in Indonesia: Transformation of worship and virtual community. *HTS Teologiese Studies / Theological Studies*, *81*(1), 1–19. https://doi.org/10.4102/hts.v81i1.10592

Moyo, M., & Pali, J. K. (2025). Christian Faith Formation and Spiritual Insecurity in Africa. *Diligentia: Journal of Theology and Christian Education*, *7*(1), 1–15. https://doi.org/10.19166/dil.v7i1.9012

Muannas, & Mansyur, M. (2020). Model Literasi Digital untuk Melawan Ujaran Kebencian di Media Sosial Digital Literacy Model to Counter Hate Speech on Social Media. *Jurnal Ilmu Pengetahuan Dan Teknologi Komunikasi*, *22*(2), 125–142. https://doi.org/10.33164/iptekkom.22.2.2020.125-142

Nagle, J. M. (2019). Learning to Leave : Expanding Shared Praxis to Understand the Religious Life and Learning of Young Catholics Beyond the Church. *Religious Education*, *114*(4), 1–16. https://doi.org/10.1080/00344087.2019.1631949

Oliver, K. M., Williams-Duncan, S., & Kimball, E. M. (2020). Digital Literacies for Ministry : A Qualitative Study of Theological Educators Preparing Students for New Media Engagement. *Ecclesial Practices*, *7*, 117–137. https://doi.org/10.1163/22144417-bja10008

Reuters. (2024). *Indonesia president orders audit of data centres after cyberattack*. Reuters. https://www.reuters.com/technology/cybersecurity/bulk-indonesia-data-hit-by-cyberattack-not-backed-up-officials-say-2024-06-28/

Rochman, F. (2024). *Dari 2017-2024, Kemenkominfo terima 572 ribu aduan terkait penipuan online*. ANTARA News Kalteng. https://kalteng.antaranews.com/berita/715351/dari-2017-2024-kemenkominfo-terima-572-ribu-aduan-terkait-penipuan-online

Salam, M., Abu Bakar, K. A., Abdul Ghani, A. T., & Mohd Aman, A. H. (2026). Cybersecurity in Higher Education Institutions Digitalisation : Addressing Threats and Vulnerabilities. *SAGE*, *16*(1), 1–14. https://doi.org/10.1177/21582440251413473

Sari, S. P., & Bermuli, J. E. (2021). Etika Kristen dalam Pendidikan Karakter dan Moral Siswa di Era Digital. *Diligentia: Journal of Theology and Christian Education*, *3*(1), 46–63. https://doi.org/10.19166/dil.v3i1.2782

Schlag, T., Frey, G., & Yadav, K. (2025). Religious Leadership and Digital Innovation : An Explorative Interview Study with Church Actors in the Swiss Context. *Religions*, *16*(491), 1–26. https://doi.org/10.3390/rel16040491

Sipahutar, M. A., Pasaribu, A. G., Sitopu, E., & Lumbantobing, L. (2025). Socio-Economic and Humanistic Aspects for Integrating Christian Ethics into the Use of Digital Technology in Christian Education : A Literature Review. *SEHATI: Socio-Economic and Humanistic Aspects for Township and Industry*, *3*(4), 800–812. https://doi.org/10.59535/sehati.v3i4.595

Smith, J. K. A. (2009). *Desiring the Kingdom: Worship, Worldview, and Formation*. Baker Academic.

Steinert, S., & Dennis, M. J. (2022). Emotions and Digital Well - Being : on Social Media's Emotional Affordances. *Philosophy & Technology*, *35*(36), 1–21. https://doi.org/10.1007/s13347-022-00530-6

Tarihoran, E., Firmanto, A. D., & Supur, A. (2024). Digital Catechesis : Embracing

Technology for Effective Faith Formation. *International Journal of Indonesian Philosophy & Theology*, *5*(1), 16–29. https://doi.org/10.47043/ijipth.v5i1.54

UNICEF. (2019). *UNICEF poll: More than a third of young people in 30 countries report being a victim of online bullying*. UNICEF. https://www.unicef.org/press-releases/unicef-poll-more-third-young-people-30-countries-report-being-victim-online-bullying

Waruwu, E. W., & Lawalata, M. (2024). Membangun Masyarakat Digital Yang Beretika: Mengintegrasikan Nilai-Nilai Kristen Di Era Teknologi Digital 5.0. *Didache: Journal of Christian Education*, *5*(1), 22–46. https://doi.org/10.46445/djce.v5i1.747

World Health Organization. (2024). *One in six school-aged children experiences cyberbullying, finds new WHO/Europe study*. WHO Regional Office for Europe. https://www.who.int/europe/news-room/27-03-2024-one-in-six-school-aged-children-experiences-cyberbullying--finds-new-who-europe-study