International Journal of Innovative Inventions in Social Science and Humanities

ISSN(print): 3050-6921, ISSN(online): 3050-693X

Volume 03 Issue 11 November 2026

DOI: 10.58806/ijiissh.2026.v3i11n14

Page No: 1678-1696

The Cybersecurity Duty of The Digital Worker: Labour Rights, Professional Obligations and The Fair Allocation of Security Risk

Dr Godwin Gaduga

Lecturer at Accra Institute of Technology Adjunct Lecturer at Blue Crest University College

ABSTRACT

When a cybersecurity incident strikes a Ghanaian organization, the investigation that follows tends to move quickly towards the last person who touched the system. The employee who clicked the link, approved the payment, or misconfigured the server becomes the visible cause of an event whose origins frequently lie in decisions taken elsewhere and earlier. This article argues that Ghanaian law already contains the materials for a more accurate allocation of responsibility, but that those materials have not been assembled for the digital workplace and are often misapplied when they are invoked. Reading the Labour Act 2003 (Act 651) together with the Cybersecurity Act 2020 (Act 1038), the Data Protection Act 2012 (Act 843), the Electronic Transactions Act 2008 (Act 772), the Evidence Act 1975 (NRCD 323) and article 24 of the 1992 Constitution, the article shows that the employer's statutory duties of training, information, safe systems of work and fair discipline must be discharged before an individual worker can fairly be found culpable, and that the Labour Act's neglected regime on loss deductions already embodies a principle of bounded and proportionate recovery. Drawing on English, South African, Canadian, German and European authority, and on the human factors literature on error and just culture, the article proposes a Contextual Security Allocation Framework. The Framework separates organizational failure from individual fault through five ordered inquiries, places evidentiary burdens on the party that controls the relevant evidence, and calibrates sanctions to a graded scale of culpability running from system-induced error to deliberate misconduct. The article concludes with eight legal principles and a set of workplace and regulatory recommendations, distinguishing throughout between what existing law requires and what reform should add.

KEYWORDS: Cybersecurity, Employment Law, Ghana, Labour Act 2003, Human Error, Just Culture, Disciplinary Fairness, Vicarious Liability, Employee Indemnity, Proportionality, Digital Evidence

ARTICLE DETAILS

Published On:
16 November 2026

Available on:
https://ijiissh.com/

I. INTRODUCTION

Every serious cybersecurity incident gives rise to two inquiries, and only one is usually conducted with rigour. The first is technical. Investigators reconstruct the intrusion path, identify the vulnerability exploited, trace the credentials used and estimate the data or funds lost. The second is normative: it asks who should answer for what happened. The technical reconstruction cannot settle that question, because the fact that a particular employee's account opened the door does not show whether the employee acted carelessly, whether the door should have been capable of being opened in that way, or whether anyone had taught the employee to recognise the threat. In practice, however, the normative inquiry often adopts the conclusions of the technical one, and the person who appears at the end of the technical chain is treated as the author of the harm.

The pattern is familiar to anyone who has advised on an incident. An accounts officer receives an email that appears to come from the managing director instructing an urgent transfer to a new supplier account, and complies. A systems administrator, working alone at a weekend because the information technology unit has two staff for an organization of four hundred, disables a firewall rule to restore a failing service and forgets to re-enable it. A customer service agent assessed on the number of calls closed each hour resets a password for a caller who sounds plausible but has not passed every verification step. A contractor engaged to migrate data leaves a database exposed to the internet. Each event can be narrated as individual failure, and in each the employer's first response may be to query, suspend, surcharge or dismiss the person concerned. Each can equally be narrated as the predictable

product of an environment in which payment approval depended on one person reading one email, security operations were understaffed, performance measures rewarded speed over verification, or a contractor was given privileged access without supervision or a defined security standard.

This article examines the ground between those two accounts. Its central question is how legal responsibility for cybersecurity incidents should be allocated between employees, contractors, managers and employers where human error, system design, inadequate training, excessive workloads or deliberate misconduct have contributed, often in combination, to the harm. The question is important for workers, who face summary dismissal, loss of end of service benefits, deductions from remuneration and provident fund balances, damage to their professional reputation in a small market and, occasionally, referral to the police. It is important for employers and regulators, because an organization that resolves every incident by removing an individual learns nothing about its own controls, discourages the prompt reporting on which incident response depends, and leaves the underlying weakness in place for the next attacker. It is also important for the coherence of Ghanaian law, since the statutes governing employment, data protection, cybersecurity and evidence each address part of the problem but have not been read together for this purpose.

Part II identifies the gap in existing scholarship. Part III sets out how security incidents occur, drawing on the human factors literature to show why the familiar contrast between 'human error' and 'technical failure' misdescribes them. Part IV maps the Ghanaian legal framework, with particular attention to sections 9, 10, 11 and 118 of the Labour Act and to the security obligations in Act 843 and Act 1038. Part V examines the employment contract and the limits of employer security policies. Part VI considers disciplinary fairness under sections 62 and 63 of the Labour Act and the Supreme Court's jurisprudence on natural justice. Part VII turns to negligence, employee indemnity and vicarious liability, and Part VIII to comparative employment law. Part IX develops the Contextual Security Allocation Framework. Parts X to XII address evidentiary burdens, sanctions and worker protections, and regulatory reform. Part XIII states the legal principles and workplace recommendations that the analysis supports, and Part XIV concludes.

Two methodological commitments run throughout. The first is that technology does not create a separate labour law; it changes the factual, evidentiary, institutional and power environment within which existing law operates.[1] The cybersecurity duty of the digital worker is therefore not a new legal category but an application of the established duties of care, fidelity and obedience to a setting that changes what those duties demand of each party. The second is to distinguish between enacted law, judicial authority, pending legislative proposals and normative recommendation, so that the reader can see at each point whether a proposition states what Ghanaian law requires or what the author contends it should require.

II. THE GAP IN EXISTING SCHOLARSHIP

The literature bearing on this problem has developed along three lines that rarely meet. The first is the human factors and usable security literature, which has argued for more than two decades that people are less the weakest link in security than the component most often asked to compensate for poorly designed systems. Adams and Sasse showed that insecure password behaviour was frequently a rational response to mechanisms that imposed unreasonable cognitive and workload demands, and that organizations which communicated poorly about risk could not fairly treat the resulting behaviour as wilful.[2] Herley later argued that much security advice imposes costs on users that exceed its expected benefit, so that ignoring it may be economically rational rather than negligent.[3] Reason's work on organizational accidents, and Dekker's development of the idea of 'just culture', supplied the concepts for distinguishing the errors that systems produce in ordinary people from the culpable choices for which individuals should answer.[4] This work is empirically grounded and directly relevant, but it is written for security engineers and safety scientists and does not engage with the legal tests by which a tribunal decides whether a dismissal was fair or a deduction lawful.

The second line is the cybersecurity law and governance literature, which has concentrated on regulatory compliance, critical information infrastructure, breach notification, corporate and director liability, and the contractual allocation of security risk between commercial parties. In Ghana, commentary on Act 1038 has understandably focused on the institutional position of the Cyber Security Authority, the licensing of service providers and practitioners, the obligations of owners of critical information infrastructure and, more recently, the proposed Cybersecurity (Amendment) Bill 2025.[5] That literature treats the organization as the

[1] Godwin Gaduga, *Contemporary and Evolving Issues in Labour Law and Practice: Workplace Governance, Digital Rights, Cybersecurity, Neurotechnology and the Future of Work* (forthcoming).

[2] Anne Adams and Martina Angela Sasse, 'Users Are Not the Enemy' (1999) 42(12) Communications of the ACM 40.

[3] Cormac Herley, 'So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users' (New Security Paradigms Workshop, Oxford, 2009).

[4] James Reason, *Human Error* (CUP 1990); James Reason, *Managing the Risks of Organizational Accidents* (Ashgate 1997); Sidney Dekker, *Just Culture: Balancing Safety and Accountability* (Ashgate 2007).

[5] Cybersecurity Act 2020 (Act 1038). The Cyber Security Authority opened public consultation on the Draft Cybersecurity (Amendment) Bill 2025 on 1 October 2025; see Digital Policy Alert, 'Ghana: Cyber Security Authority Opened Consultation on

unit of analysis and asks what it owes to regulators, customers and the public. It seldom addresses how an organization that has failed may lawfully distribute that failure among the people who work within it.

The third line is Ghanaian employment law scholarship, which has produced a substantial body of commentary on wrongful and unfair termination, natural justice in disciplinary proceedings, the relationship between contractual and statutory protection, and remedies before the courts and the National Labour Commission. That commentary is strong on procedure and on the grounds of fair termination in section 62 of the Labour Act. It has not yet considered how 'incompetence' and 'proven misconduct' should be understood where the alleged failing is a security lapse occurring in an environment that the employer designed and controlled. Nor has it examined section 70 of the Act, which permits loss deductions caused by a worker only on demanding conditions, as a source of principle for the allocation of security losses.

Comparative employment law offers partial assistance. English law retains the House of Lords' decision in *Lister v Romford Ice and Cold Storage Co Ltd*, which recognized an employer's right to an indemnity from a negligent employee, alongside a settled practice of not enforcing it.[6] German law has developed, through the Federal Labour Court, a doctrine of graduated employee liability that limits recovery according to the degree of fault because the employer organizes the work and bears its operational risk.[7] South African law structures misconduct and incapacity dismissals through a statutory Code of Good Practice that asks whether the employee knew, or could reasonably be expected to have known, the rule allegedly breached.[8] None of these has been adapted to the features of cybersecurity incidents, in which causation is distributed across technical and human layers, the evidence is held almost entirely by the employer, and the triggering act is often induced by an adversary deliberately exploiting predictable human responses.

The gap can therefore be stated precisely. So far as the author is aware, there is no sustained scholarly treatment, in Ghana or in comparable common law African jurisdictions, of the allocation of responsibility for cybersecurity incidents within the employment relationship that integrates labour law, negligence, evidence and cybersecurity regulation, and that offers courts, the National Labour Commission and employers a structured method for distinguishing individual culpability from organizational failure. This article supplies such a method, grounds it in Ghanaian authority wherever possible, and identifies the points at which reform is needed.

III. HOW SECURITY INCIDENTS OCCUR

A legal framework for allocating responsibility must begin from an accurate account of how incidents happen, because a rule built on a false picture of causation will distribute blame falsely however carefully it is applied. Reason's model of organizational accidents is the most useful starting point. It distinguishes active failures, which are the unsafe acts of people at the operational edge of a system and whose effects are felt almost immediately, from latent conditions, which are the decisions of designers, managers and procurers that lie dormant until they combine with an active failure to produce harm.[9] A successful phishing email is an active failure. The absence of multi-factor authentication on the email system, a payment process that allows a single officer to release funds on an emailed instruction, a decision not to fund security training, and a staffing level that leaves the officer processing forty payments before noon are latent conditions. The legal significance of the distinction is that active failures are visible and attributable to a named individual, whereas latent conditions are diffuse, historical and attributable, if at all, to institutional choices that no disciplinary charge can capture. A system of responsibility that examines only the visible layer will consistently overstate the fault of workers and understate that of organizations.

For legal purposes, it is useful to distinguish five contributing sources, present in varying proportions in almost every incident. The first is human error in the strict sense: an unintended deviation from what the person intended or ought to have done, whether a slip of attention, a lapse of memory or a mistake of judgment made in good faith. Such errors are a normal property of human cognition; their frequency can be reduced by design but never eliminated by exhortation.[10] The second is system design, which includes the architecture of technical controls, the configuration of access rights, the presence or absence of verification steps and the interface through which security decisions are presented. A system that allows a junior officer to approve a large transfer without a second approver is designed to convert a single error into a loss. The third is training and information: whether the worker was told what the risks were, how to recognise them, what the employer's rules required and why. The fourth is workload and working conditions, which affect the likelihood of error through fatigue, time pressure, interruption and the incentives created by performance

Draft Cybersecurity (Amendment) Bill' <https://digitalpolicyalert.org> accessed 6 November 2026; GhanaFact, 'Draft 2025 Cybersecurity Bill: CSA's New Functions, Police Powers and Other Major Amendments' (11 November 2025) <https://ghanafact.com> accessed 6 November 2026.

[6] *Lister v Romford Ice and Cold Storage Co Ltd* [1957] AC 555 (HL).

[7] Bundesarbeitsgericht (Großer Senat), Beschluss vom 27 September 1994, GS 1/89 (A).

[8] Labour Relations Act 66 of 1995 (South Africa), sch 8, Code of Good Practice: Dismissal, item 7.

[9] Reason, *Human Error* (n 4) ch 7.

[10] Reason, *Human Error* (n 4).

measurement. The fifth is deliberate misconduct, ranging from knowing breach of a clear security rule for convenience, through the sharing of credentials, to malicious insider action such as data theft or sabotage.

These sources interact, and their interaction is what makes legal allocation difficult. Workload pressure alters the character of a rule violation. A worker who bypasses a verification step to meet a target that management knows cannot be met while complying with every step has made a choice, but its moral and legal weight is heavily conditioned by the employer's own decisions. Where a shortcut is tolerated, rewarded, or modelled by supervisors, it becomes the working norm, and the formal rule survives only on paper, a process that organizational sociologists have described as the normalization of deviance.[11] Training interacts with design in the same way. Training cannot compensate for an environment that demands constant vigilance; an employer that trains staff to detect phishing but leaves them exposed to hundreds of unfiltered external emails a day has transferred to them a detection task that its technology should perform.

Cybersecurity incidents also differ from ordinary workplace accidents in a legally important respect. In an industrial accident, the hazard is indifferent to the worker; a machine does not study its operator. In a cybersecurity incident, the hazard is often an intelligent adversary who has studied the organization, impersonated its leadership, timed the attack to coincide with periods of pressure, and crafted the message to exploit the deference to authority and willingness to help that employers otherwise value in their staff. Business email compromise and social engineering succeed because they are designed to deceive the reasonable person, not only the careless one. The question whether a worker 'should have known' cannot therefore be answered by asking whether the deception is detectable with hindsight and a forensic report. It must be answered by asking what a reasonable worker in that role, with that training, under those conditions and facing that quality of deception, would have done at the time.

It follows that the legal inquiry must be ordered. Before asking whether the worker fell below the standard expected, a tribunal must ask what standard the employer's own arrangements made it reasonable to expect, because the content of the worker's duty of care is partly determined by the system in which the worker was placed. Part IX develops this ordering principle.

IV. THE GHANAIAN LEGAL FRAMEWORK

A. The constitutional foundation

Article 24(1) of the 1992 Constitution guarantees every person the right to work under satisfactory, safe and healthy conditions. The guarantee has conventionally been read in physical terms, but its language is not confined to bodily safety. A working environment in which a worker is exposed, without adequate tools or training, to skilled adversaries whose success will be attributed to the worker personally is not satisfactory or safe in any ordinary sense. Article 24(1) therefore lends constitutional weight to the proposition that the employer's duty to provide a safe system of work extends to the digital systems through which work is now performed. Where the employer is a public body, article 23 requires administrative bodies and officials to act fairly and reasonably and to comply with the requirements imposed on them by law, which brings disciplinary decisions following security incidents within the constitutional standard of administrative justice.[12] Article 18(2), which protects the privacy of correspondence and communication subject to lawful and necessary interference, governs the investigation, since the evidence used to attribute an incident to an individual is usually drawn from monitoring that individual's communications and system activity.[13]

B. The reciprocal duties in the Labour Act

Sections 8 to 11 of the Labour Act contain a compact statement of reciprocal rights and duties that has received little analytical attention. Section 8 confirms the employer's rights to discipline and terminate employment and to formulate policies, but expressly makes those rights subject to the Act and to any other enactment. Section 9 imposes duties directly relevant to cybersecurity. The employer must provide work and appropriate materials, machinery, equipment and tools (section 9(a)); take all practicable steps to ensure that the worker is free from risk of personal injury or damage to health in the course of employment (section 9(c)); develop human resources by training and retraining workers (section 9(d)); and provide and ensure the operation of an adequate procedure for discipline (section 9(e)). Section 10 confers corresponding rights on the worker, including the rights to work under satisfactory, safe and healthy conditions, to a reasonable limitation of working hours, to be trained and retrained, and to receive information relevant to the work.

Section 11 sets out the worker's duties. The most relevant are the duties to work conscientiously (section 11(a)); to exercise due care in the execution of assigned work (section 11(d)); to obey lawful instructions regarding the organization and execution of work (section 11(e)); to protect the interests of the employer (section 11(g)); and to take proper care of the employer's property entrusted to the worker or under the worker's immediate control (section 11(h)). An employer disciplining a worker for a security lapse will

[11] Diane Vaughan, *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA* (University of Chicago Press 1996).

[12] Constitution of the Republic of Ghana 1992, arts 23 and 24(1).

[13] ibid art 18(2).

typically rely on sections 11(d), 11(e) and 11(h), treating the lapse as a failure of due care, disobedience of a security instruction, or a failure to protect entrusted property such as credentials, devices and data.

Sections 9 and 11 are not independent lists. They are reciprocal obligations within a single relationship, and the content of the worker's duty under section 11 depends in part on whether the employer has performed its duties under section 9. The duty to exercise due care in assigned work presupposes that the work has been assigned with appropriate tools, information and training. The duty to obey lawful instructions presupposes that instructions have been given, communicated intelligibly and made capable of performance within the time and resources allowed. The duty to take proper care of entrusted property presupposes that the employer has explained what proper care of a digital asset requires when its vulnerabilities are invisible to the ordinary user. This reading follows from the text. Section 11 opens with the words 'without prejudice to the provisions of this Act', which include section 9, and section 8 makes the employer's disciplinary rights subject to the Act as a whole.

C. Occupational safety and the safe system of work

Part XV of the Labour Act reinforces the point. Section 118(1) requires every employer to ensure that every worker works under satisfactory, safe and healthy conditions, and section 118(2)(a) requires the employer to provide and maintain a plant and system of work that are safe and without risk to health. Section 118(2)(c) requires the employer to provide the necessary information, instructions, training and supervision, having regard to the age, literacy level and other circumstances of the worker. Failure to discharge these obligations without reasonable excuse is an offence under section 118(5).[14] The provisions were drafted with physical hazards in mind, and it would overstate the position to say that they presently impose a criminal obligation to maintain secure information systems. The concept of a 'system of work' is, however, understood at common law to include the organization of tasks, the sequence of operations and the provision of supervision, and the duty to supply information and training suited to the circumstances of the worker states in statutory form the principle that the human factors literature has established for security. Section 118(2)(c) is particularly significant because it ties the adequacy of training to the circumstances of the individual worker, so that a single generic awareness video cannot be assumed to discharge the duty for every category of staff.

Section 119 is also relevant. A worker who has reasonable cause to believe that a situation presents an imminent and serious danger to life, safety or health must report it and may remove himself or herself from it, and the employer may not dismiss the worker or withhold remuneration for doing so. The provision concerns physical danger, but its logic, which protects a worker who declines to continue with unsafe work, provides a useful analogy for a worker who declines to execute an instruction that appears fraudulent, or who halts a process because a security warning has appeared, and is then disciplined for the delay. Part XII recommends that the analogy be made explicit.

D. Data protection and cybersecurity legislation

The Data Protection Act places the security obligation on the data controller. Section 28 requires the controller to secure the integrity of personal data in its possession or control by adopting appropriate, reasonable, technical and organizational measures to prevent loss, damage, unauthorized destruction and unlawful access or processing.[15] The statute treats organizational measures, which include staff training, access management and supervision, as part of the controller's own obligation. When an employee's error leads to a breach, the controller cannot discharge its regulatory responsibility by identifying the employee; from the regulator's perspective, the error is evidence bearing on whether the controller's organizational measures were appropriate. Section 29 applies where processing is carried out by a processor, which is the position of many contractors and outsourced technology providers, and requires the controller to ensure that the processor establishes and complies with security safeguards.

The Cybersecurity Act operates at a different level. It establishes the Cyber Security Authority, provides in sections 35 to 40 for the designation of critical information infrastructure, and imposes on owners of designated infrastructure obligations of compliance, audit and incident reporting.[16] It also provides for the licensing of cybersecurity service providers and the accreditation of cybersecurity establishments and professionals. Two features of Act 1038 bear on internal allocation. Its obligations fall on the institution that owns or operates the relevant system, which confirms that security is an organizational duty. And section 1(2) directs that the Act be read together with other enactments, including the Electronic Transactions Act, the Electronic Communications Act and the Data Protection Act, which supports the integrated reading proposed here.[17] The Cybersecurity (Amendment) Bill 2025,

[14] Labour Act 2003 (Act 651), s 118(5).

[15] Data Protection Act 2012 (Act 843), s 28.

[16] Act 1038, ss 35 to 40 and 47.

[17] ibid s 1(2).

which would substantially enlarge the Authority's powers and has attracted considerable public criticism, is not law, and it is referred to below only as an indication of the direction of policy.[18]

E. Whistleblowing and protected disclosure

The Whistleblower Act 2006 (Act 720) protects employees who disclose in good faith impropriety that includes conduct endangering public safety or causing economic loss, and prohibits victimization through dismissal, suspension, harassment or other detriment.[19] Its relevance to cybersecurity lies at the boundary between reporting the security failings of colleagues or the organization and reporting one's own error. Act 720 protects the former where its conditions are met. It does not in terms protect a worker who reports his or her own mistake. That gap is significant because the speed of containment depends on prompt self-reporting, which workers will not offer if every report becomes the evidential basis of their own dismissal.

V. THE EMPLOYMENT CONTRACT: IMPLIED DUTIES, SECURITY POLICIES AND THEIR LIMITS

A. The implied duties and their digital content

The common law of employment, received into Ghanaian law and operating alongside the Labour Act, implies into every contract of employment a duty of fidelity, a duty to obey lawful and reasonable orders, and a duty to exercise reasonable care and skill. Each has security content. Fidelity forbids deliberate disclosure of confidential information, misuse of access for personal ends and sabotage of the employer's systems. Obedience requires compliance with lawful security instructions. Care requires the competence reasonably to be expected of a person in the role. The duties differ in structure. Fidelity concerns loyalty and intention, so that breach ordinarily requires knowledge or deliberate wrongdoing. Obedience concerns the response to a communicated instruction, so that breach presupposes an instruction that was clear, lawful, reasonable and actually communicated. Care concerns the quality of performance against an objective standard, so that breach depends on what a reasonable worker in the same position would have done.

This structure corresponds to the account of incidents in Part III. Deliberate misconduct engages fidelity and justifies the most serious consequences. Knowing breach of a clear rule engages obedience. Inadvertent error engages, at most, the duty of care, and whether it amounts to a breach cannot be decided without examining the conditions that the employer created. A common failure in disciplinary practice is to merge these categories into a single charge of 'negligence' or 'gross misconduct', which attaches to inadvertent error the opprobrium and sanction appropriate to betrayal.

B. Security policies as lawful instructions

Most Ghanaian employers of any size maintain an information security policy, an acceptable use policy, and rules on passwords, devices and data handling. Their legal status varies. Where a policy is incorporated into the contract of employment or the applicable collective agreement, its terms bind as contractual terms, and section 105(2) of the Labour Act provides that the terms of a collective agreement concerning personal obligations of workers are to be regarded as terms of the individual contract.[20] Where a policy is not incorporated, it may still operate as a body of lawful instructions within section 11(e), provided that it is lawful, reasonable, within the scope of the employment and actually communicated to the worker. Section 12(2), which requires a contract of employment to express the rights and obligations of the parties in clear terms, supports the conclusion that obligations on which an employer intends to rely for discipline must be stated clearly.

Communication is the condition most often unmet. A policy uploaded to an intranet, acknowledged by a click during induction and never explained cannot fairly be said to have been communicated to a worker for whom its technical language is opaque. The South African Code of Good Practice, discussed in Part VIII, makes the worker's knowledge of the rule, or the reasonableness of expecting such knowledge, an express element of fair dismissal for misconduct. The same principle is implicit in the Ghanaian requirement that misconduct be 'proven', since an employer cannot prove that a worker disobeyed a rule that the worker had no fair opportunity to understand.

Reasonableness is the second condition. Security rules that cannot be observed while meeting the performance requirements the employer imposes at the same time are not reasonable instructions in their application, even if each is reasonable in isolation. If an employer requires call-back verification of every change to supplier bank details but sets processing targets that make call-back impossible within working hours, the instruction to verify has been qualified in practice by the instruction to process, and a worker who prioritizes the latter has resolved a contradiction the employer created rather than disobeyed the employer. Sections 33 and 35

[18] See n 5; International IDEA, 'Democracy Tracker: Ghana, October 2025' <https://www.idea.int/democracytracker> accessed 6 November 2026.

[19] Whistleblower Act 2006 (Act 720).

[20] Act 651, s 105(2).

of the Labour Act, which fix maximum working hours at eight a day or forty a week except as the Act provides and restrict compulsory overtime, supply a statutory baseline against which the reasonableness of a security workload can be judged.

C. Contractual clauses shifting security losses to the worker

Some employers now include clauses making workers personally liable for losses arising from security breaches, or authorizing deductions from salary or terminal benefits to make good such losses. These clauses must be read subject to Part IX of the Labour Act. Section 69(2)(a) prohibits the imposition of a pecuniary penalty on a worker for any cause whatsoever, and section 69(2)(b) prohibits deductions from remuneration except as permitted by section 70 or other law. Section 70(1)(e) permits a deduction, with the worker's consent, to meet a loss suffered by the employer through the loss of or damage to property used in connection with, or produced by, the employer's business and under the worker's control. Section 70(2) then imposes four cumulative conditions. The employer must be satisfied that the loss or damage was caused by the worker and that the worker is clearly shown to be responsible; that the amount is fair and does not exceed the actual or fairly estimated loss; that the worker has had a reasonable opportunity to show cause why the deduction should not be made; and that the rate of deduction avoids hardship to the worker and his or her dependents. A worker aggrieved by a deduction may complain to the National Labour Commission under section 70(3).

Two points follow. The first concerns drafting. In the consolidated text, section 70(2) attaches its conditions to deductions under 'subsection (1)(f)', the paragraph dealing with deductions made in compliance with an order of the Commission, rather than to paragraph (e), which concerns loss and damage.[21] Read literally, the protective conditions would govern Commission orders, which do not need them, and not employer deductions for loss, which plainly do. The conditions themselves, which refer to loss or damage 'caused by the worker' and to the worker's responsibility, make sense only in relation to paragraph (e). The better view, consistent with a purposive reading of protective labour legislation and with the object of Part IX, is that the reference is a clerical error for paragraph (e), and that every employer deduction for loss must satisfy all four conditions.

The second point concerns substance. Even on that reading, section 70 is a narrow gateway. It requires consent; it requires that the worker be 'clearly shown to be responsible', which demands more than contribution; and it imports proportionality in both amount and rate. A clause in a standard form contract signed at the start of employment can hardly supply consent to a deduction whose amount and circumstances are then unknown, and the safer construction is that consent must relate to the specific deduction. More fundamentally, the requirement that the worker be clearly shown to be responsible calls for the contextual inquiry proposed in this article. A worker whose error was the active failure in an incident made possible by latent organizational conditions has contributed to the loss but is not, on any fair analysis, clearly shown to be responsible for all of it. The facts of *Oduro v Graphic Communication Group Ltd*, in which the employer's dismissal letter alleged negligence of duty and causing financial loss, surcharged the worker and another person with the sum said to have been lost, and deducted part of that sum from the worker's provident fund contributions, show how readily these measures are combined in Ghanaian practice.[22]

D. Contractors, agency workers and managers

The problem changes shape for workers who are not employees in the ordinary sense. Independent contractors fall outside the protective provisions of the Labour Act, and their responsibility for security failures is governed by their contracts and by the law of negligence. Where a contractor processes personal data on the employer's behalf, the contractor is a processor, and Act 843 requires the controller to ensure that the processor complies with security safeguards. A controller that engages a contractor without defining security obligations has therefore itself failed to discharge a statutory duty. The author has examined elsewhere the contractual allocation of security risk between commercial parties.[23] The narrower point here is that an employer cannot rely on the absence of a contractual security standard to shift to an individual contractor a loss that a properly drafted engagement would have allocated, priced and insured. Temporary workers employed continuously for six months or more are treated as permanent workers by section 75(1) of the Labour Act and enjoy the general disciplinary protections, but workers engaged for a specified period or specified work, probationers and casual workers are excluded from Part VIII by section 66.

Managers occupy a distinct position. A manager may be excluded from trade union membership by section 79(2) because of the managerial or confidential nature of the role, but remains a worker for the purposes of Part VIII. More importantly, managers are frequently the authors of the latent conditions that make incidents possible. They set workloads, approve or refuse budgets for security tools and training, design approval processes, and model or tolerate shortcuts. A coherent framework must therefore be able

[21] Act 651, s 70(2), as it appears in the consolidated text published by the Ghana Legal Information Institute <https://ghalii.org/akn/gh/act/2003/651> accessed 6 November 2026.

[22] *Oduro v Graphic Communication Group Ltd* [2018] GHASC 74 (12 December 2018), Civil Appeal No J4/25/2018, facts as recited in the judgment of Benin JSC.

[23] Godwin Gaduga, 'The Cybersecurity Warranty Gap: Representations, Indemnities and Risk Allocation in Technology Transactions' (forthcoming).

to attribute responsibility upwards as well as downwards, and should treat a manager's failure to implement or resource security controls within his or her area of authority as a potential breach of that manager's own duty of care.

VI. DISCIPLINARY FAIRNESS AFTER AN INCIDENT

A. The statutory grounds and the employer's burden

Section 62 of the Labour Act provides that termination is fair if it is effected on one of four grounds, two of which are relevant here: that the worker is incompetent or lacks the qualification for the work for which he or she is employed (section 62(a)), and the proven misconduct of the worker (section 62(b)). Section 63(4) provides that a termination may be unfair if the employer fails to prove that the reason for it is fair or that it was made in accordance with a fair procedure or the Act. The burden of justification therefore rests on the employer as to both substance and procedure. Section 15(e) separately recognises termination for inability to work by reason of incompetence or proven misconduct, and the Supreme Court has consistently held that an employer which proceeds through its disciplinary machinery must establish good grounds and observe both its own procedures and the rules of natural justice.[24]

The choice between the two grounds is more than a matter of labelling. Incompetence under section 62(a) concerns capability: the worker cannot perform the work to the required standard. Misconduct under section 62(b) concerns culpable conduct: the worker could have acted properly but chose, or carelessly failed, to do so. A single inadvertent security lapse by a worker whose performance is otherwise satisfactory is rarely evidence of incompetence, and it is misconduct only if it reflects a culpable failure of care rather than the ordinary fallibility that every system must anticipate. Repeated lapses after training and warning may evidence incapacity, but the fair response to incapacity is ordinarily instruction, support and an opportunity to improve. Section 9(d), which places on the employer the duty of training and retraining, makes that principle part of Ghanaian law even though the Act prescribes no performance improvement procedure. Conversely, a worker who deliberately disables a security control, shares credentials in breach of a clear and understood rule, or removes data without authority has committed misconduct of the gravest kind, and the incompetence ground does not apply.

The word 'proven' in section 62(b) deserves emphasis. Misconduct must be established as a fact on evidence, not suspected or inferred from the occurrence of a loss. A security incident is not itself proof of misconduct, because, as Part III has shown, incidents occur in well-run organizations staffed by careful people. The employer must prove both what the worker did and that it fell below the standard reasonably to be expected in the circumstances.

B. Natural justice in the Supreme Court's jurisprudence

The Supreme Court has developed consistent authority on the procedural requirements of disciplinary action. In *Aboagye v Ghana Commercial Bank,* it held a bank employee's dismissal void because the bank had departed from its own disciplinary procedures and from the rules of natural justice, emphasizing that an employer which prescribes a procedure must follow it.[25] In *Awuku-Sao v Ghana Supply Co Ltd,* the Court accepted that written responses to a draft forensic audit could, in the circumstances, satisfy the right to be heard, and that summary dismissal was lawful where misconduct was objectively established, while again stressing the obligation to follow the employer's own procedures.[26] In *Gavor v Bank of Ghana,* the Court held that an employer may summarily dismiss for proven gross misconduct notwithstanding the employee's subsequent acquittal in criminal proceedings, and that an opportunity to answer before an investigatory committee could satisfy the requirement of a hearing.[27]

These decisions establish a flexible conception of the hearing, which need not resemble a trial, but they also establish that the flexibility operates within a structure of fairness that cannot be dispensed with. Three features of that structure are especially important in cybersecurity cases. First, the worker must be told with sufficient particularity what is alleged. The employer must identify the act or omission said to constitute misconduct and the rule or standard said to have been breached; a charge of 'causing a security breach' describes an outcome, not conduct, and is not an allegation of misconduct at all. Secondly, the worker must have a genuine opportunity to answer, which in a technical case requires access to the evidence relied on, including relevant logs and forensic findings, since a worker cannot rebut an attribution he or she has never seen. Thirdly, the decision maker must be free from the appearance of bias. This requires particular vigilance where the investigation is conducted by the information technology or security function whose own controls are implicitly in question, since that function has an institutional interest in locating the cause elsewhere.

---

[24] *Aboagye v Ghana Commercial Bank* [2001-2002] SCGLR 797; *Awuku-Sao v Ghana Supply Co Ltd* [2009] GHASC 21 (11 March 2009).

[25] *Aboagye* (n 24).

[26] *Awuku-Sao v Ghana Supply Co Ltd* [2009] GHASC 21 (11 March 2009), Civil Appeal No J4/15/2008.

[27] *Gavor v of Bank Ghana* [2014] GHASC 190 (27 November 2014), Civil Appeal No 14/4/2014.

C. Investigation, interdiction and timing

Incident response and disciplinary process pursue different objectives and should be sequenced accordingly. In the hours after detection, the priority is containment, and it may be entirely appropriate to suspend a worker's access, preserve devices and accounts, and interdict the worker pending investigation. Section 29 of the Labour Act contemplates suspension pending disciplinary or criminal proceedings and preserves the leave entitlement of a worker who is later reinstated. Containment measures must not, however, be treated as findings, and no disciplinary conclusion should be reached before the root cause analysis is complete. A decision taken before the employer knows why its controls failed is taken without evidence relevant to the worker's culpability, because the adequacy of those controls forms part of the standard against which the worker's conduct is measured.

D. Consistency and the tolerated shortcut

Fairness also requires consistency. An employer that has tolerated a practice, such as sharing a departmental login because of a shortage of licences, or approving payments on emailed instructions while the managing director is travelling, cannot fairly discipline one worker for following that practice on the occasion when it is exploited. Where management knew of a widespread deviation and did nothing, the deviation has become part of the system of work, and the rule it contradicts is, for disciplinary purposes, waived or at least suspended until clearly reinstated. The South African Code makes consistent application of the rule a condition of fair dismissal, and the principle reflects a general requirement of equal treatment that Ghanaian tribunals are well placed to apply.

VII. NEGLIGENCE, INDEMNITY AND VICARIOUS LIABILITY

A. The standard of care and the professional worker

Where an employer seeks to recover its loss from a worker rather than merely to discipline, the question becomes one of civil liability, and the standard is that of the reasonable person in the worker's position. The standard is objective, but its content is shaped by the role, the knowledge reasonably expected of someone performing it, and the circumstances of the act. For workers who hold themselves out as having specialist skill, the standard rises accordingly. The test in *Bolam v Friern Hospital Management Committee*, under which a professional is judged by the standard of a responsible body of practitioners skilled in the relevant field, is the natural reference point for systems administrators, security analysts and developers.[28] Its application in Ghana is reinforced by the accreditation of cybersecurity professionals under Act 1038, which presupposes that recognized standards of professional competence exist. A security engineer who leaves a production database exposed without authentication may be judged by what a competent security engineer would have done. An accounts officer deceived by a skilled impersonation is judged by what a reasonable accounts officer, not a forensic investigator, would have recognized.

The professional obligations of digital workers are not uniform. The cybersecurity duty of a frontline user is principally to follow intelligible rules, to report what seems wrong, and not to circumvent controls deliberately. The duty of a technical professional is broader: it includes exercising professional judgment, escalating risks the professional is not authorised or resourced to address, and refusing to implement configurations known to be unsafe. The duty of a manager includes the duty to resource and supervise. A framework that applies a single standard of 'security awareness' to every worker will be too demanding of some and too lenient of others.

B. The employer's indemnity and its practical limits

In *Lister v Romford Ice and Cold Storage Co Ltd,* the House of Lords held, by a majority, that an employee who negligently injured a third party in the course of employment had broken an implied contractual duty of care owed to the employer and was liable to indemnify the employer for the damages it had paid.[29] The decision has not been overruled and, as part of the received common law, is capable of applying in Ghana. Its practical force has nonetheless been severely limited. In England, the decision led to an interdepartmental inquiry, after which insurers agreed not to pursue subrogated claims against employees in the absence of collusion or wilful misconduct. In *Morris v Ford Motor Co Ltd,* the Court of Appeal refused to allow an employer's indemnifier to enforce a *Lister* claim by subrogation against an employee, holding that such a claim was unrealistic in modern industrial conditions and that an implied term excluded it.[30] English law has thus moved towards recognizing that the employer, which organizes the work, profits from it and can insure against its risks, is the appropriate bearer of losses arising from the ordinary negligence of its workforce.

That development supports a cautious approach to *Lister* in Ghana, at least in the cybersecurity context. *Lister* concerned a single act of negligent driving, an activity over whose risks the employee had direct control and to which the employer had contributed little. Cybersecurity incidents present almost the opposite configuration. The worker's control over the risk is partial and mediated

[28] *Bolam v Friern Hospital Management Committee* [1957] 1 WLR 582 (QB).

[29] *Lister* (n 6).

[30] *Morris v Ford Motor Co Ltd* [1973] QB 792 (CA).

by systems the employer designs; the employer's contribution through latent conditions is substantial; and the employer is far better placed to insure, through cyber insurance policies that are now widely available. Unrestricted indemnity claims against workers in these circumstances would invert the allocation of risk that the employment relationship justifies. The Labour Act's treatment of loss deductions in section 70, with its requirements of clear responsibility, a fair amount and the avoidance of hardship, expresses a legislative policy of bounded recovery that a Ghanaian court may properly take into account in determining the scope of any implied indemnity at common law.

C. Apportionment and the employer's own fault

Where a loss results from the combined fault of worker and employer, the Civil Liability Act 1963 (Act 176) provides the statutory machinery for apportioning liability between concurrent wrongdoers and for reducing damages on account of a claimant's own fault.[31] The significance of this machinery for the present problem has received little attention. An employer that sues a worker for a security loss is in substance a claimant whose own negligence in designing, resourcing and supervising its systems has contributed to the harm. Even where the worker is found negligent, the employer's recovery should be reduced to reflect its own share of responsibility. Apportionment under the general law thus reinforces the conclusion that section 70 reaches within employment law: an employer cannot convert its own organizational failure into a debt owed by its staff.

D. Vicarious liability and the malicious insider

The problem also has an external dimension. Where a worker's act causes loss to a third party, such as a customer whose data is disclosed, the employer may be vicariously liable if the wrongful act was so closely connected with the work the employee was authorised to do that it may fairly and properly be regarded as done in the course of employment. In *Various Claimants v WM Morrison Supermarkets plc,* the United Kingdom Supreme Court held that an employer was not vicariously liable for a disgruntled employee's deliberate online disclosure of payroll data, because the employee was pursuing a personal vendetta rather than engaging, however misguidedly, in the employer's business.[32] The decision confirms that deliberate malicious conduct by an insider is treated differently from negligent performance of the job, which supports the graded approach to culpability proposed below. It also shows that the absence of vicarious liability for a rogue insider does not end the employer's exposure, because the employer remains subject to its own primary duties as data controller. Under Act 843, the obligation to adopt appropriate organizational measures is the controller's own, so the question of whether the controller adequately restricted and monitored the insider's access concerns the controller's compliance, not the insider's motive.

VIII. COMPARATIVE EMPLOYMENT LAW

Comparative material is used here not as authority binding on Ghanaian courts but as evidence of how developed labour law systems have responded to the features that cybersecurity incidents share with older problems of workplace fault.

A. England and Wales: reasonable belief and the range of reasonable responses

English unfair dismissal law asks whether the employer genuinely believed in the employee's misconduct, whether it had reasonable grounds for that belief, and whether it had carried out as much investigation as was reasonable in the circumstances, a formulation derived from *British Home Stores Ltd v Burchell*.[33] The sanction is then tested against the range of reasonable responses open to a reasonable employer, following *Iceland Frozen Foods Ltd v Jones*.[34] The *Burchell* inquiry is valuable because it makes the adequacy of the investigation part of fairness, and an investigation into a security incident that does not examine the employer's own controls is an inadequate investigation into whether the employee was at fault. The range of reasonable responses test is more problematic, because its deference to the employer's judgment risks entrenching the reflex of individual blame that this article criticizes. A Ghanaian tribunal applying section 63(4), which places the burden of proving fairness on the employer, is not bound to adopt that deference and should not do so.

B. South Africa: knowledge of the rule and the distinction from incapacity

South Africa's Labour Relations Act 1995 is supplemented by a Code of Good Practice: Dismissal, set out in Schedule 8. Its guidelines on misconduct direct the decision maker to consider whether the employee contravened a workplace rule, whether the rule was valid or reasonable, whether the employee was aware or could reasonably be expected to have been aware of it, whether it had been consistently applied, and whether dismissal was an appropriate sanction.[35] Separate guidelines on poor work performance

[31] Civil Liability Act 1963 (Act 176).

[32] *Various Claimants v WM Morrison Supermarkets plc* [2020] UKSC 12, [2020] AC 989.

[33] *British Home Stores Ltd v Burchell* [1980] ICR 303 (EAT).

[34] *Iceland Frozen Foods Ltd v Jones* [1983] ICR 17 (EAT).

[35] Labour Relations Act 66 of 1995 (n 8) sch 8, item 7.

require appropriate evaluation, instruction, training, guidance or counselling, and a reasonable period for improvement, before dismissal.[36] In *Sidumo v Rustenburg Platinum Mines Ltd,* the Constitutional Court held that a commissioner deciding the fairness of a dismissal must form his or her own view rather than defer to the employer, while giving due weight to the employer's reasons.[37] The South African model institutionalizes two distinctions drawn in this article: between misconduct and incapacity, and between a rule that exists on paper and a rule that the worker could fairly be expected to know.

C. Canada: contextual proportionality

In *McKinley v BC Tel,* the Supreme Court of Canada rejected the proposition that any act of dishonesty automatically justifies summary dismissal. The question is whether, in context, the misconduct was such that the employment relationship could no longer viably continue, and the sanction must be proportionate to the nature and degree of the misconduct.[38] The contextual approach was developed in relation to dishonesty, but its logic applies with greater force to security lapses, which are seldom dishonest. A rule that a single security error automatically justifies dismissal would be even less defensible than the rule rejected in *McKinley*.

D. Germany: graduated employee liability

German law has the most developed doctrine on the allocation of loss within the employment relationship. In its decision of 27 September 1994, the Grand Senate of the Federal Labour Court confirmed that the principles limiting employee liability apply to all work that is occasioned by the business and performed in the course of the employment relationship, abandoning the earlier restriction to work classified as dangerous.[39] Under the resulting doctrine of internal loss adjustment (innerbetrieblicher Schadensausgleich), an employee who causes damage through slight negligence is ordinarily not liable at all. Damage caused through medium negligence is shared between employer and employee according to the circumstances, including the risk inherent in the activity, the employee's remuneration and the availability of insurance. Only in cases of gross negligence or intent does the employee ordinarily bear the full loss, and even then, the courts have in some cases limited liability where the loss is grossly disproportionate to the employee's earnings. The doctrine rests on the recognition that the employer organizes the work, sets its conditions and bears its operational risk, so that losses arising from the ordinary imperfection of human performance belong to the enterprise. It is the clearest comparative expression of the principle of bounded recovery that section 70 of the Ghanaian Labour Act contains in compressed form.

E. European human rights law and cybersecurity regulation

Two strands of European law bear on the evidentiary and regulatory aspects of the problem. In *Bărbulescu v Romania,* the Grand Chamber of the European Court of Human Rights held that monitoring of an employee's communications must be accompanied by adequate and sufficient safeguards, including prior notice of the possibility and extent of monitoring, a legitimate reason, consideration of less intrusive means and proportionality in the use made of the results.[40] In *López Ribalda v Spain,* the Grand Chamber accepted that covert video surveillance could be justified in narrowly defined circumstances of reasonable suspicion of serious misconduct, while emphasizing proportionality.[41] These decisions provide a persuasive structure for applying article 18(2) of the Ghanaian Constitution and the principles of Act 843 to the investigation of security incidents. Separately, Directive (EU) 2022/2555 (the NIS 2 Directive) requires the management bodies of essential and important entities to approve cybersecurity risk management measures, to oversee their implementation and to be capable of being held liable for infringements; it also requires members of those bodies to follow training and the entities to offer similar training to employees regularly.[42] The Directive places accountability for the organization's security posture at the level of management and treats staff training as an organizational obligation rather than a personal burden.

F. International labour standards

The International Labour Organization's Termination of Employment Convention 1982 (No 158) requires a valid reason connected with the capacity or conduct of the worker or the operational requirements of the undertaking, and an opportunity for the worker to answer allegations before termination for reasons of conduct or performance. It also provides for the burden of proving a valid

[36] ibid items 8 and 9.

[37] *Sidumo v Rustenburg Platinum Mines Ltd* [2007] ZACC 22, 2008 (2) SA 24 (CC).

[38] *McKinley v BC Tel* 2001 SCC 38, [2001] 2 SCR 161.

[39] BAG GS 1/89 (A) (n 7).

[40] *Bărbulescu v Romania* App no 61496/08 (ECtHR, Grand Chamber, 5 September 2017).

[41] *López Ribalda v Spain* App nos 1874/13 and 8567/13 (ECtHR, Grand Chamber, 17 October 2019).

[42] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union [2022] OJ L333/80, arts 20 and 21.

reason to be placed on the employer, as one of the options available to Member States.[43] Sections 62 and 63(4) of the Labour Act closely reflect these principles. In 2022, the International Labour Conference added a safe and healthy working environment to the fundamental principles and rights at work and designated the Occupational Safety and Health Convention 1981 (No 155) and the Promotional Framework for Occupational Safety and Health Convention 2006 (No 187) as fundamental conventions.[44] That development strengthens the argument that the employer's duty to provide a safe system of work is a matter of fundamental labour rights and extends to risks created by the digital organization of work.

IX. THE CONTEXTUAL SECURITY ALLOCATION FRAMEWORK

The preceding analysis yields materials rather than a method. Ghanaian law supplies reciprocal duties in sections 9 and 11 of the Labour Act, a safe system of work obligation in section 118, an employer burden of proof in section 63(4), a protective regime for loss deductions in section 70, apportionment under Act 176, and an organizational security obligation under Act 843. Comparative law supplies graduated liability, knowledge of the rule, contextual proportionality and management accountability. The human factors literature supplies the distinction between active failures and latent conditions. What is lacking is an ordered procedure by which a disciplinary panel, the National Labour Commission or a court can apply these materials to a particular incident without merging organizational failure into individual blame, or excusing genuine misconduct on the ground that no system is perfect. The Contextual Security Allocation Framework is proposed for that purpose. It consists of five inquiries undertaken in sequence, and its defining feature is that the examination of the organization precedes any finding about the individual, because the answers to that examination set the standard against which the individual is judged.

A. First inquiry: characterisation of the incident

The first inquiry separates three matters that are routinely conflated: the outcome, meaning the harm that occurred; the technical pathway, meaning how the adversary or failure produced the harm; and the human acts or omissions that formed part of that pathway. Only the last can be the subject of a disciplinary allegation, and each such act must be identified precisely, together with the person who performed it, the time and context, and the evidence on which its attribution rests. An incident that cannot be resolved into identified acts by identified persons cannot found individual discipline, although it may well require organizational remediation.

B. Second inquiry: organizational preconditions

The second inquiry asks whether the employer had discharged its own duties in relation to the risk that materialized. It examines five matters. The first is design: whether the technical and procedural controls were proportionate to a known or reasonably foreseeable threat, so that, for example, a payment process exposed to impersonation required independent verification of changes to bank details. The second is training and information: whether the worker had received instruction specific to the role and the threat, intelligible in light of the worker's circumstances within the meaning of section 118(2)(c), and sufficiently recent to be relevant. The third is resourcing and workload: whether the worker had the time, staffing and tools to comply with security requirements alongside the other demands of the role. The fourth is the clarity and consistency of rules: whether the rule allegedly breached was clearly stated, actually communicated and consistently enforced, including against managers. The fifth is supervision: whether the employer exercised the oversight the risk warranted, including review of privileged access and of contractors.

This inquiry precedes the next because the worker's standard of care is partly determined by its answers. It does not follow that every organizational deficiency excuses every worker. The inquiry produces a finding as to whether a material deficiency existed and whether it was causally related to the act in question, and that finding conditions, without necessarily determining, the assessment of the individual's conduct.

C. Third inquiry: classification of individual conduct

The third inquiry classifies the worker's conduct on a graded scale of culpability. The scale adapts the distinctions developed in safety science to the legal categories of the employment contract and is set out in Table 1.

Table 1: Graded scale of culpability

Level	Conduct	Illustration	Duty engaged	Presumptive response
1. System induced error	An error that the design, workload or training made likely for any reasonable worker in the role	An officer approves a spoofed transfer under a single-approver process with no call-back control and a same-day target	None breached; the deficiency is organisational	No sanction; organisational remediation and support for the worker

[43] ILO Termination of Employment Convention 1982 (No 158), arts 4, 7 and 9.

[44] ILO Declaration on Fundamental Principles and Rights at Work 1998, as amended by the International Labour Conference in 2022.

Level	Conduct	Illustration	Duty engaged	Presumptive response
2. Inadvertent slip	A genuine lapse of attention or judgment within an adequate system	A trained officer with a working call-back process omits the call on one occasion	Care (s 11(d)), at most a minor breach	Coaching or retraining; no disciplinary record for a first occurrence
3. At-risk choice	A knowing departure from a rule without appreciation of the risk, often normalised in the workplace	A team routinely shares a login because licences are short, and the shared credential is phished	Obedience (s 11(e)), qualified by the employer's tolerance	Corrective instruction; a warning only if the rule was clear and enforced; managerial accountability for the tolerance
4. Reckless disregard	Conscious disregard of a known and substantial risk without justification	An administrator disables logging and multi-factor authentication to save time, despite an express prohibition and training	Care and obedience, seriously breached	Formal warning up to dismissal, depending on the harm and context; organisational deficiencies may mitigate
5. Deliberate misconduct	Intentional wrongdoing, dishonesty, malice or collusion	An insider sells customer data or plants malicious code	Fidelity; the criminal law may be engaged	Summary dismissal, subject to proof and fair procedure; civil recovery and criminal referral available

Classification depends on what the worker knew, intended and could reasonably have recognized, assessed as at the time of the act and not with the benefit of the forensic report. The sophistication of the adversary is relevant here: a deception engineered to defeat a reasonable person cannot support a finding that the person deceived acted unreasonably.

D. Fourth inquiry: causal contribution

The fourth inquiry asks how much of the harm is fairly attributable to the individual act rather than to the organizational deficiency. Two counterfactual questions structure it. Would the loss have occurred, or been as severe, if the worker had acted properly? Would it have occurred, or been as severe, if the deficiency identified in the second inquiry had not existed? Where a reasonable control would have prevented or contained the loss notwithstanding the worker's act, the organizational deficiency is the dominant cause, and the worker's contribution is correspondingly reduced. This inquiry is the natural place for apportionment under Act 176 and for the requirement in section 70(2) that the worker be 'clearly shown to be responsible'.

E. Fifth inquiry: proportionate response

The fifth inquiry selects the response. The presumptive responses in Table 1 are starting points, to be adjusted in light of the causal finding, the harm caused, the worker's record and candour, and the need for consistent treatment. Three rules govern the adjustment. First, where the second inquiry has identified a material and causally related organizational deficiency, conduct at levels 1 and 2 should attract no disciplinary sanction, and conduct at level 3 should attract corrective rather than punitive measures. Secondly, conduct at level 4 may justify serious sanction notwithstanding organizational deficiencies, but those deficiencies are a mitigating factor that a fair decision maker must weigh. Thirdly, conduct at level 5 is not mitigated by organizational deficiencies for disciplinary purposes, because the duty of fidelity does not depend on the quality of the employer's systems, although those deficiencies remain relevant to the employer's own regulatory and civil exposure. The Framework thus preserves the employer's legitimate interest in enforcing security requirements against those who knowingly disregard them, while declining to treat the ordinary fallibility of people working within deficient systems as a disciplinary matter.

X. EVIDENTIARY BURDENS

A. The statutory allocation

The Evidence Act distinguishes the burden of persuasion from the burden of producing evidence, provides that the burden of persuasion in civil matters generally requires proof by a preponderance of the probabilities, and allocates to each party the burden of persuasion as to each fact essential to the claim or defence it asserts.[45] Section 13(1) adds that, in any civil or criminal action, the burden of persuasion as to the commission by a party of a crime which is directly in issue requires proof beyond reasonable doubt.[46] In employment cases, section 63(4) of the Labour Act places on the employer the burden of proving that the reason for termination

[45] Evidence Act 1975 (NRCD 323), ss 10, 11, 12 and 14.

[46] ibid s 13(1).

was fair and that a fair procedure was followed. The result is a coherent allocation. The employer must prove the conduct alleged, that it amounted to misconduct or incompetence, and that the procedure was fair. Where the allegation is one of deliberate wrongdoing amounting to a crime, such as unauthorized access, data theft or fraud, and the crime is directly in issue in civil proceedings, the higher standard applies.

The decision in *Gavor* that an employer may dismiss for proven gross misconduct despite the employee's acquittal in criminal proceedings is consistent with this analysis.[47] An acquittal shows only that the prosecution did not discharge its burden in the criminal court; it does not prevent the employer from proving misconduct in the employment forum. The employer must nevertheless prove it there, and where the misconduct alleged is itself criminal in character, section 13(1) governs the standard of proof if the matter is litigated.

B. Unequal access to evidence

The defining evidentiary feature of cybersecurity disputes is the almost complete imbalance in access to evidence. The employer controls the logs, email gateway records, endpoint telemetry, access management records, configuration history, training records, staffing data and incident reports, and often retains external forensic investigators whose reports are commissioned for its own purposes. The worker usually has only his or her own recollection. This imbalance has two consequences.

First, it justifies placing on the employer the burden of producing evidence on the second inquiry. Once a worker contends, with some foundation, that the incident was made possible by inadequate design, training, resourcing, rule clarity or supervision, the employer should be required to produce the evidence relevant to that contention, because it alone holds it. This does not reverse the burden of persuasion; it applies the principle that the burden of producing evidence may shift to the party with peculiar knowledge of the facts in issue. It is also implicit in section 63(4), since an employer that has not examined its own controls has not proved that its reason for dismissal was fair.

Secondly, the imbalance raises the importance of preserving evidence. An employer that wipes devices, overwrites logs or fails to retain the forensic data on which its own conclusions rest, and then relies on those conclusions against a worker, invites the inference that the missing evidence would not have supported it. The maxim omnia praesumuntur contra spoliatorem, applied in *Armory v Delamirie*, states a principle of general application that a Ghanaian tribunal may properly invoke.[48]

C. Attribution and authentication of digital evidence

The attribution of a security event to an individual rests almost always on digital records, and those records prove less than they appear to. A log entry shows that an account acted. It does not show that the person to whom the account was issued performed it, because credentials may have been stolen, shared, or phished, or used by malware operating within the user's session. Section 22 of the Electronic Transactions Act, which governs the attribution of data messages, and section 136 of the Evidence Act, which requires evidence sufficient to sustain a finding that a record is what its proponent claims, must therefore be applied with care.[49] Section 7 of Act 772 directs attention, in assessing the evidential weight of an electronic record, to the reliability of the manner in which it was generated, stored and communicated, the manner in which its integrity was maintained, and the manner in which its originator was identified.[50] Each of these factors is open to genuine dispute in a security incident, where the integrity of the system is the very matter in question. A disciplinary panel that treats an account-level log as conclusive proof of individual conduct, without considering whether the account was compromised, has not applied the attribution and weight provisions that Ghanaian law prescribes.

D. Monitoring evidence and its limits

In insider cases, much of the evidence will come from monitoring the worker's activity. Article 18(2) of the Constitution permits interference with the privacy of correspondence and communication only in accordance with law and as necessary for the purposes it specifies, and Act 843 requires personal data to be processed lawfully, in a reasonable manner, for a specific and lawful purpose of which the data subject is aware, and with minimality.[51] Taking the *Bărbulescu* safeguards as a persuasive guide, monitoring evidence should be relied on in disciplinary proceedings where the worker had prior notice of the possibility and nature of monitoring, the monitoring served a legitimate security purpose and was proportionate to it, and less intrusive means were considered. The point is not that improperly obtained evidence is necessarily excluded, a question on which Ghanaian courts retain discretion, but that the manner in which evidence was obtained is relevant to the fairness of the procedure that section 63(4) requires the employer to prove.

---

[47] *Gavor* (n 27).

[48] *Armory v Delamirie* (1722) 1 Str 505, 93 ER 664.

[49] Electronic Transactions Act 2008 (Act 772), s 22; NRCD 323, s 136.

[50] Act 772, s 7.

[51] Constitution 1992, art 18(2); Act 843, ss 17 to 19, 22 and 23.

XI. PROPORTIONATE SANCTIONS AND WORKER PROTECTIONS

A. Proportionality as a requirement of fairness

The Labour Act contains no express requirement that disciplinary sanctions be proportionate, but proportionality is implicit in its structure. Section 63(4) requires the employer to prove that the reason for termination was fair, and a reason that would justify a warning does not become a fair reason for dismissal merely because it is genuine. Section 70(2) requires loss deductions to be fair in amount and imposed at a rate that avoids hardship. The Supreme Court has also accepted structured proportionality reasoning in an employment context as part of constitutional analysis.[52] A sanction grossly disproportionate to the culpability of the conduct and to its contribution to the harm is therefore, on the better view, not merely harsh but unfair within the meaning of the Act.

Proportionality here has three dimensions. The first is proportionality to culpability, which the scale in Table 1 is designed to capture: the same outcome may result from conduct at any of the five levels, and the sanction should follow the level rather than the outcome. The second is proportionality to causal contribution, so that a worker whose act was a minor element in an incident dominated by organizational deficiencies is not sanctioned as its author. The third is proportionality to the totality of consequences. The decision maker should consider the combined effect of dismissal, loss of terminal benefits, deductions, adverse references and criminal referral, rather than treating each as a separate decision. The facts of *Oduro*, in which dismissal, surcharge and a provident fund deduction were imposed together, show how quickly these consequences accumulate.[53]

B. A safe harbour for self-reporting

The most valuable single protection that law and workplace policy can offer is a safe harbour for prompt self-reporting. Incident response depends on speed. A worker who realizes within minutes that he or she has entered credentials into a fraudulent page, or approved a payment that now seems suspicious, can enable containment that saves the organization far more than any sanction could recover. A worker who expects to be dismissed for reporting will delay, conceal, or hope the matter passes unnoticed. Experience in aviation and healthcare has shown that reporting systems work only where those who report their own honest errors are protected from punitive consequences while remaining accountable for reckless or deliberate conduct.[54] Ghanaian law provides no such safe harbour. Act 720 protects disclosures of impropriety but is not framed around self-reporting, and nothing in the Labour Act prevents an employer from using a worker's own report as the principal evidence against him or her.

This article proposes that a prompt and candid self-report of conduct at levels 1 to 3 should, as a matter of workplace policy now and of regulation in due course, preclude disciplinary sanction for that conduct, and that a self-report of conduct at level 4 should be a significant mitigating factor. Even without regulation, a tribunal assessing the fairness of a sanction may treat an employer's failure to give weight to a prompt self-report as relevant to proportionality. An employer that has published a reporting policy promising non-punitive treatment and then departs from it will also encounter the principle in *Aboagye* that an employer must follow its own procedures.

C. Limits on financial consequences

The Labour Act already sets firm limits on financial consequences, and the task is chiefly to apply them. Pecuniary penalties are prohibited by section 69(2)(a), and loss deductions are permitted only within the conditions of section 70, read as explained in Part V. A surcharge imposed in a dismissal letter, which purports to create a debt owed by the worker, must be analyzed either as an exercise of the section 70 power, in which case its conditions apply, or as a claim to an indemnity at common law, in which case the employer must prove negligence, causation and loss ordinarily and accept apportionment for its own fault under Act 176. In neither case may an employer simply declare that a worker owes it the value of an incident. Provident fund balances and other terminal entitlements require particular protection, because their seizure is often the most severe financial consequence a worker suffers and is frequently effected without any adjudication.

D. Protection against retaliation and the refusal of unsafe instructions

A duty to follow safety rules must be accompanied by protection for workers who do so at the cost of speed or convenience. A worker who will not release a payment until a call-back has been completed, who declines to disable a control at a manager's request, or who reports that a system is unsafe should not suffer for it. Section 119 of the Labour Act protects a worker who removes himself or herself from imminent and serious danger, and Act 720 protects good faith disclosure of impropriety. Together they support a broader principle that a worker may not be disciplined for complying with a security requirement, for reasonably refusing to execute an instruction that appears fraudulent or unsafe, or for raising a security concern in good faith. That principle should be stated in workplace policies and, in due course, in regulations.

---

[52] *Civil and Local Government Staff Association of Ghana (CLOGSAG) v Attorney-General* [2017] GHASC 18.

[53] *Oduro* (n 22).

[54] Dekker (n 4).

E. Parity for contractors and outsourced personnel

Contractors who are not employees fall outside the Labour Act, but fairness and good governance support extending the substance of these protections to them by contract. An organization that applies a just culture to its employees but treats contractors as dispensable will find that contractors, who often hold privileged technical access, are the least likely to report their own errors. The engagement terms of any contractor with security responsibilities should define the expected security standard, the training and access provided, the incident reporting obligation, and the basis on which the contractor's liability for security loss is limited, insured or excluded.

XII. REGULATORY REFORM

Much of what this article proposes can be achieved within existing law by courts, the National Labour Commission and employers who read the statutes together and apply them with attention to context. Some matters require regulatory action, either because the existing text is defective or because the necessary protections cannot be derived from it with sufficient certainty. The proposals below are arranged by the institution best placed to act.

Parliament. The reference in section 70(2) of the Labour Act to 'subsection (1)(f)' should be corrected to refer to paragraph (e), so that the conditions of clear responsibility, fair amount, opportunity to show cause and avoidance of hardship unambiguously govern every employer deduction for loss. Parliament should also consider providing expressly that terminal benefits and provident fund balances may not be applied to an alleged loss without either the worker's specific written consent, given after the loss has been quantified, or an order of the Commission or a court.

The Minister responsible for labour. Section 121 of the Labour Act empowers the Minister to make regulations prescribing specific measures to safeguard the health and safety of workers. That power can support regulations on the digital working environment that would confirm that the duty in section 118(2)(c) to provide information, instructions, training and supervision extends to the security risks inherent in the worker's tasks; require security training to be role-specific and periodically refreshed; and recognise, by analogy with section 119, a worker's right to pause a process or decline an instruction that reasonably appears fraudulent or unsafe without suffering detriment.

The National Labour Commission. The Commission's power under section 152 to make regulations on its procedures, together with its adjudicative function under section 64, makes it well placed to issue guidance on complaints arising from security incidents. That guidance could adopt the five inquiries of the Framework, confirm that the employer's burden under section 63(4) includes producing evidence on organizational preconditions, and state the Commission's approach to section 70 deductions.

The Cyber Security Authority. The Authority's directives to owners of critical information infrastructure, and any guidance it issues to the wider economy, should treat workforce security as an organizational obligation. A code on workforce security could require designated institutions to keep role-specific training records, to operate non-punitive channels for reporting honest error, and to include an assessment of organizational preconditions in every incident report, so that the regulator's own data capture latent conditions as well as the active failures that are easiest to record. If the Cybersecurity (Amendment) Bill 2025 proceeds, its provisions on cyber hygiene and accountability should attach accountability to the management of regulated institutions, as article 20 of the NIS 2 Directive does, rather than transferring it to individual staff.

The Data Protection Commission. The Commission should state in guidance that a data controller does not discharge its obligation under section 28 of Act 843 by identifying and disciplining the employee whose act triggered a breach, and that in every case of human error it will assess the controller's training, access controls and supervision.

Employers and trade unions. Section 98 of the Labour Act permits collective agreements to address conditions of work, including occupational health and safety measures, and discipline. The social partners should negotiate security incident protocols that give effect to the Framework: a non-punitive reporting channel, root cause analysis before any disciplinary decision, access to relevant evidence, joint review of training and workload, and limits on financial recovery. Because section 105(4) prevents individual workers from waiving rights conferred by a collective agreement, such protocols would have a durability that unilateral employer policies lack.

Public sector employers. For public bodies, the requirement of administrative justice in article 23 of the Constitution strengthens each of these proposals. The Office of the Head of Civil Service, the Public Services Commission and comparable bodies should issue service-wide guidance applying the Framework to public servants, many of whom work with outdated systems and limited security support and are therefore especially exposed to being blamed for organizational deficiencies.

XIII. LEGAL PRINCIPLES AND WORKPLACE RECOMMENDATIONS

A. Eight legal principles

The analysis supports eight principles. Each is accompanied by an indication of whether it states existing law, an interpretation of existing law, or a proposal for reform.

1. **Reciprocal duty.** A worker's duties of care, obedience and protection of the employer's property under section 11 of the Labour Act are to be construed in light of the employer's duties under sections 9 and 118 to provide tools, training, information, safe systems and supervision. A worker is not in breach of a duty whose performance the employer's own default made unreasonably difficult. (Interpretation of existing law.)
2. **Organizational priority.** In disciplinary or civil proceedings arising from a security incident, the adequacy of the employer's design, training, resourcing, rule clarity and supervision must be examined before the individual worker's culpability is determined, because those matters partly determine the standard of care against which the worker is judged. (Interpretation of existing law, grounded in section 63(4).)
3. **The reasonable digital worker.** The standard of care is that of a reasonable worker in the same role, with the same training and resources, facing the same quality of deception at the time of the act, and not that of a forensic investigator with hindsight. Technical professionals are judged by the standard of competent practitioners in their field. (Existing law of negligence.)
4. **Graded culpability.** Conduct contributing to a security incident is to be classified by reference to the worker's knowledge and intention, distinguishing system-induced error, inadvertent slip, at-risk choice, reckless disregard and deliberate misconduct, and the sanction should follow the classification rather than the outcome. (Interpretation of 'proven misconduct' in section 62(b), supported by comparative law.)
5. **Bounded recovery.** An employer may recover a security loss from a worker only where the worker is clearly shown to be responsible, in an amount that is fair and reflects apportionment for the employer's own fault, and at a rate that avoids hardship. Pecuniary penalties are prohibited. (Existing law under sections 69 and 70 and Act 176; legislative correction of section 70(2) recommended.)
6. **Evidential integrity.** The employer bears the burden of producing evidence on organizational preconditions, must preserve the digital evidence on which it relies, must disclose that evidence to the worker in time for the worker to answer, and may not treat account-level activity as proof of individual conduct without considering whether the account was compromised. (Interpretation of existing law under section 63(4), NRCD 323 and Act 772.)
7. **Protected reporting and compliance.** A worker who promptly and candidly reports his or her own honest error, complies with a security requirement at the cost of productivity, reasonably refuses an instruction that appears fraudulent or unsafe, or raises a security concern in good faith, must not suffer detriment for doing so. (Partly existing law by analogy with section 119 and Act 720; regulatory reform recommended.)
8. **Managerial accountability.** Managers who control the workloads, budgets, processes and supervision that shape security risk owe a duty of care in respect of those matters, and responsibility for incidents arising from deficiencies within their authority is to be attributed to them rather than displaced onto subordinate staff. (Interpretation of existing duties of care, reinforced by comparative regulation.)

B. Workplace recommendations

For employers, these principles translate into measures that can be adopted without legislative change.

- Publish a security incident policy that explains the five levels of culpability, commits the organization to examining its own controls before reaching conclusions about individuals, and states the consequences attached to each level.
- Separate incident response from discipline. State expressly that containment measures, including suspension of access, are not disciplinary, and take no disciplinary decision until a root cause analysis addressing organizational preconditions is complete.
- Ensure that investigators are independent of the controls under review. Where the information technology or security function designed the controls that failed, the disciplinary inquiry should be led or reviewed by someone outside that function.
- Provide training that is specific to each role, intelligible to the workers concerned, periodically refreshed and recorded, so that its adequacy can be demonstrated.
- Remove single points of human failure. High-risk actions, such as changes to supplier bank details, large payments, privileged configuration changes and bulk data exports, should require independent verification that does not depend on one person's vigilance.
- Review performance targets to ensure that security procedures can be followed within the working hours permitted by sections 33 to 35 of the Labour Act.
- Operate a non-punitive channel for reporting honest errors and near misses, and make its protection known.
- Give a worker facing allegations arising from an incident the relevant logs and findings, allow the worker to be accompanied by a representative and, in technical cases, to obtain independent technical advice.

- Confine financial recovery to section 70 and its conditions, never apply terminal benefits or provident fund balances to an alleged loss without specific consent or adjudication, and insure the organization's cyber risk rather than treating staff as its insurers.
- Include in every contractor engagement term defining security standards, access, training, reporting obligations and the limits of the contractor's liability.
- Hold managers accountable through performance objectives that include the security of the processes they own and the adequacy of the resources they allocate.

XIV. CONCLUSION

The digital worker owes a cybersecurity duty, and nothing in this article is intended to dilute it. Workers who deliberately misuse their access, sell data, sabotage systems or knowingly disable controls that protect colleagues and customers betray the trust on which the employment relationship depends. Ghanaian law rightly permits their summary dismissal, their pursuit in damages and, where the facts warrant it, their prosecution. Employers are entitled to enforce the duties of care, obedience and fidelity in the digital workplace.

What Ghanaian law does not permit, when its provisions are read together and in light of their purposes, is the conversion of organizational failure into individual guilt. The Labour Act constructs the employment relationship as a structure of reciprocal duties, in which the worker's obligation of due care is matched by the employer's obligations to provide tools, training, information, a safe system of work and an adequate disciplinary procedure, and in which the employer must prove the fairness of both its reason and its procedure. The same statute prohibits pecuniary penalties and permits recovery of loss only where the worker is clearly shown to be responsible, and only in fair and bearable amounts. The Data Protection Act and the Cybersecurity Act place the security obligation on the institution. The Evidence Act and the Electronic Transactions Act require attribution to be proved and digital records to be weighed according to their reliability. The Constitution guarantees satisfactory, safe and healthy working conditions and, in the public sector, fair and reasonable administrative action.

The Contextual Security Allocation Framework gives these materials a usable form. By requiring the organizational inquiry to precede the individual one, by classifying conduct according to culpability rather than outcome, by weighing causal contribution, and by requiring sanctions to be proportionate in their combined effect, it aims to produce allocations of responsibility that are both accurate and fair. It also serves the employer's own interest, since an organization that learns from its incidents, encourages staff to report their mistakes and invests in controls rather than scapegoats will be more secure than one that does not. Courts, the National Labour Commission, regulators and employers already have the means to ensure that, after the next incident, the first question is not simply who clicked the link, but what the organization had done to make that click safe.

REFERENCES

1) Godwin Gaduga, Contemporary and Evolving Issues in Labour Law and Practice: Workplace Governance, Digital Rights, Cybersecurity, Neurotechnology and the Future of Work (forthcoming).
2) Anne Adams and Martina Angela Sasse, 'Users Are Not the Enemy' (1999) 42(12) Communications of the ACM 40.
3) Cormac Herley, 'So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users' (New Security Paradigms Workshop, Oxford, 2009).
4) James Reason, Human Error (CUP 1990); James Reason, Managing the Risks of Organizational Accidents (Ashgate 1997); Sidney Dekker, Just Culture: Balancing Safety and Accountability (Ashgate 2007).
5) Cybersecurity Act 2020 (Act 1038). The Cyber Security Authority opened public consultation on the Draft Cybersecurity (Amendment) Bill 2025 on 1 October 2025; see Digital Policy Alert, 'Ghana: Cyber Security Authority Opened Consultation on Draft Cybersecurity (Amendment) Bill' <https://digitalpolicyalert.org> accessed 6 November 2026; GhanaFact, 'Draft 2025 Cybersecurity Bill: CSA's New Functions, Police Powers and Other Major Amendments' (11 November 2025) <https://ghanafact.com> accessed 6 November 2026.
6) Lister v Romford Ice and Cold Storage Co Ltd [1957] AC 555 (HL).
7) Bundesarbeitsgericht (Großer Senat), Beschluss vom 27 September 1994, GS 1/89 (A).
8) Labour Relations Act 66 of 1995 (South Africa), sch 8, Code of Good Practice: Dismissal, item 7.
9) Reason, Human Error (n 4) ch 7.
10) Reason, Human Error (n 4).
11) Diane Vaughan, The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA (University of Chicago Press 1996).
12) Constitution of the Republic of Ghana 1992, arts 23 and 24(1).
13) ibid art 18(2).
14) Labour Act 2003 (Act 651), s 118(5).

15) Data Protection Act 2012 (Act 843), s 28.
16) Act 1038, ss 35 to 40 and 47.
17) ibid s 1(2).
18) See n 5; International IDEA, 'Democracy Tracker: Ghana, October 2025' <https://www.idea.int/democracytracker> accessed 6 November 2026.
19) Whistleblower Act 2006 (Act 720).
20) Act 651, s 105(2).
21) Act 651, s 70(2), as it appears in the consolidated text published by the Ghana Legal Information Institute <https://ghalii.org/akn/gh/act/2003/651> accessed 6 November 2026.
22) Oduro v Graphic Communication Group Ltd [2018] GHASC 74 (12 December 2018), Civil Appeal No J4/25/2018, facts as recited in the judgment of Benin JSC.
23) Godwin Gaduga, 'The Cybersecurity Warranty Gap: Representations, Indemnities and Risk Allocation in Technology Transactions' (forthcoming).
24) Aboagye v Ghana Commercial Bank [2001-2002] SCGLR 797; Awuku-Sao v Ghana Supply Co Ltd [2009] GHASC 21 (11 March 2009).
25) Aboagye (n 24).
26) Awuku-Sao v Ghana Supply Co Ltd [2009] GHASC 21 (11 March 2009), Civil Appeal No J4/15/2008.
27) Gavor v of Bank Ghana [2014] GHASC 190 (27 November 2014), Civil Appeal No 14/4/2014.
28) Bolam v Friern Hospital Management Committee [1957] 1 WLR 582 (QB).
29) Lister (n 6).
30) Morris v Ford Motor Co Ltd [1973] QB 792 (CA).
31) Civil Liability Act 1963 (Act 176).
32) Various Claimants v WM Morrison Supermarkets plc [2020] UKSC 12, [2020] AC 989.
33) British Home Stores Ltd v Burchell [1980] ICR 303 (EAT).
34) Iceland Frozen Foods Ltd v Jones [1983] ICR 17 (EAT).
35) Labour Relations Act 66 of 1995 (n 8) sch 8, item 7.
36) ibid items 8 and 9.
37) Sidumo v Rustenburg Platinum Mines Ltd [2007] ZACC 22, 2008 (2) SA 24 (CC).
38) McKinley v BC Tel 2001 SCC 38, [2001] 2 SCR 161.
39) BAG GS 1/89 (A) (n 7).
40) Bărbulescu v Romania App no 61496/08 (ECtHR, Grand Chamber, 5 September 2017).
41) López Ribalda v Spain App nos 1874/13 and 8567/13 (ECtHR, Grand Chamber, 17 October 2019).
42) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union [2022] OJ L333/80, arts 20 and 21.
43) ILO Termination of Employment Convention 1982 (No 158), arts 4, 7 and 9.
44) ILO Declaration on Fundamental Principles and Rights at Work 1998, as amended by the International Labour Conference in 2022.
45) Evidence Act 1975 (NRCD 323), ss 10, 11, 12 and 14.
46) ibid s 13(1).
47) Gavor (n 27).
48) Armory v Delamirie (1722) 1 Str 505, 93 ER 664.
49) Electronic Transactions Act 2008 (Act 772), s 22; NRCD 323, s 136.
50) Act 772, s 7.
51) Constitution 1992, art 18(2); Act 843, ss 17 to 19, 22 and 23.
52) Civil and Local Government Staff Association of Ghana (CLOGSAG) v Attorney-General [2017] GHASC 18.
53) Oduro (n 22).
54) Dekker (n 4).