UNIT 4

The **Consumer Protection Act, 2019**, is a legislative framework in India aimed at safeguarding the rights of consumers and providing them a speedy mechanism to resolve disputes. It replaced the Consumer Protection Act, 1986, to address emerging challenges in e-commerce, direct selling, and misleading advertisements.

Objectives of the Consumer Protection Act, 2019:

1. **Protection of Consumer Interests**:
   - Safeguard consumers from unfair trade practices and exploitation.
2. **Establishment of Consumer Rights**:
   - Ensure consumers have access to accurate information, choice, and redressal mechanisms.
3. **Efficient Dispute Resolution**:
   - Provide timely and effective resolution of consumer disputes via dedicated redressal agencies.
4. **Promotion of Consumer Awareness**:
   - Empower consumers with the knowledge to make informed decisions.
5. **Regulation of E-commerce and Misleading Ads**:
   - Address grievances arising in the digital marketplace and curb deceptive practices.

Machinery for Consumer Protection:

The Act establishes a three-tier quasi-judicial system for the resolution of consumer disputes :

Consumer Disputes Redressal Commissions (CDRCs)

A. District Consumer Disputes Redressal Commission (DCDRC)

- **Jurisdiction**:
  - Handles disputes where the value of goods/services and compensation claimed does not exceed ₹1 crore.
- **Role**:
  - Hears cases related to defective goods, deficiency in services, overcharging, unfair trade practices, etc.
- **Appeals**:
  - Decisions can be appealed to the State Commission within 45 days.

B. State Consumer Disputes Redressal Commission (SCDRC)

- **Jurisdiction**:
  - Hears disputes involving claims between ₹1 crore and ₹10 crore.
  - Handles appeals from the District Commission.
- **Role**:
  - Acts as an intermediary appellate authority and also handles specific cases of significant monetary value.
- **Appeals**:
  - Decisions can be appealed to the National Commission within 30 days.

C. National Consumer Disputes Redressal Commission (NCDRC)

- **Jurisdiction**:
    - Handles disputes where the value exceeds ₹10 crore.
    - Acts as an appellate authority for decisions from the State Commission.
- **Role**:
    - The apex body for consumer disputes in India.
    - Ensures consistency in judgments across lower commissions.
- **Appeals**:
    - Final appeals can be made to the Supreme Court of India within 30 days.

Defects and Deficiency Removal:

1. **Defect in Goods**:
    - A defect refers to any fault, imperfection, or shortcoming in the quality, quantity, or performance of a product.
    - Remedies: Replacement, repair, or refund.
2. **Deficiency in Services**:
    - A deficiency involves any shortfall in the nature, manner, or quality of performance of a service.
    - Remedies: Compensation, refund, or performance of service as agreed.

Rights of Consumers Under the Consumer Protection Act, 2019

The **Consumer Protection Act, 2019**, ensures that consumers in India are empowered to safeguard their interests. It enshrines **six fundamental rights**, inspired by global principles outlined by the United Nations.

1. Right to Safety

- Consumers have the right to be protected against the marketing of goods and services that are hazardous to life and property.
- Example: Safety standards for electrical appliances, food products, and drugs to prevent harm.

2. Right to Information

- Consumers have the right to be informed about the quality, quantity, potency, purity, standard, and price of goods or services.
- This enables consumers to make informed decisions and avoid being deceived.
- Example: Detailed labeling on packaged goods, disclosures in advertisements.

3. Right to Choose

- Consumers have the right to access a variety of goods and services at competitive prices without being subjected to restrictive trade practices.
- Example: Freedom to select service providers in telecom or choose between multiple brands.

4. Right to Be Heard

- Consumers have the right to voice grievances and seek solutions in appropriate forums.
- Ensures that complaints and concerns are considered seriously by sellers, manufacturers, and regulatory bodies.
- Example: Filing complaints in consumer forums for defective products or poor services.

5. Right to Seek Redressal

- Consumers are entitled to seek compensation or other remedies for unfair trade practices, exploitation, or defective goods and services.
- Example: Replacement of defective goods, refund for substandard services, or compensation for loss.

6. Right to Consumer Education

- Consumers have the right to acquire knowledge and skills to make informed and confident choices regarding goods and services.
- Example: Government campaigns like **"Jago Grahak Jago"** aim to educate consumers about their rights and responsibilities.

The Right to Information (RTI) Act of 2005 is a significant piece of legislation in India that empowers citizens to access information from public authorities. Enacted on 15th June 2005, this Act promotes transparency, accountability, and good governance by granting citizens the right to seek information about government bodies' activities and decisions.

Key Provisions of the RTI Act

Scope of Access:
The Act allows any citizen, including Non-Resident Indians (NRIs), to request information related to government policies, programs, expenditures, and other official actions.

Coverage:
It applies to central, state, and local government bodies, as well as NGOs receiving substantial government funding.
Response.

Mechanism:
Public authorities are obligated to respond to RTI requests within a specified timeframe, with certain exemptions for information affecting national security, personal privacy, or commercial interests.

Objectives of the RTI Act

Transparency:
To foster openness and accountability in government operations.

Citizen Empowerment:
To enable citizens to participate effectively in the democratic process.

Corruption Prevention:
To curb corruption by making government actions more transparent.

Good Governance:
To improve responsiveness and efficiency in government departments.

Efficiency:
To encourage more effective functioning of government entities.

Importance of the RTI Act :

Democratic Right:
Supports the fundamental right to freedom of speech and expression.

Citizen Empowerment:
Enhances informed public participation in governance.

Accountability:
Allows citizens to hold public authorities accountable.

Anti-Corruption:
Acts as a key measure to uncover and prevent corrupt practices.

Development and Progress:
Ensures effective use of government resources, benefiting public welfare.

Judicial and Administrative Reforms:
The RTI Act has driven significant improvements in government processes, making them more responsive and efficient

The Right to Information Act, 2005: Salient Features and Coverage

The *Right to Information (RTI) Act, 2005* was enacted in India to promote transparency and accountability in the functioning of public authorities. It empowers citizens to request information from public authorities, ensuring that governmental actions are open to scrutiny and that the people have a right to access public documents.

Here are the key features and provisions of the RTI Act:

Salient Features of the RTI Act, 2005:

1. Right to Information:
The Act provides the citizens of India with the right to access information under the control of public authorities. This includes records, documents, emails, samples, models, and any other material held by public authorities.

2. Public Authorities:

The Act applies to all public authorities, which include government bodies at the central, state, and local levels, as well as other organizations substantially funded or controlled by the government.

3. Designation of Public Information Officers (PIOs):
Public authorities are required to appoint Public Information Officers (PIOs) who are responsible for providing requested information within the stipulated time frame.

4. Time-bound Responses:
The Act mandates that information requested must be provided within 30 days of receiving the request, except in cases relating to the life and liberty of a person (which requires a response within 48 hours).

5. Exemptions:
Certain types of information are exempt from disclosure, such as matters related to national security, sovereignty, relations with foreign countries, and information that could affect the integrity of the country.

6. Appeals and Penalties:
If the requested information is not provided or is incorrectly denied, citizens can appeal to a higher officer within the same public authority or to the Information Commission, which is empowered to impose penalties.

Coverage of the RTI Act:

The RTI Act covers information related to:

1. Public Authorities:
This includes central and state government bodies, public sector undertakings, local government institutions, and non-governmental organizations funded or controlled by the government.

2. Information Held by Public Authorities:
It covers information in any form such as documents, records, emails, opinions, contracts, and decisions made by public authorities.

3. Access to Information:
Citizens can request information from public authorities, and these authorities are required to provide the information unless it falls under the exempt categories.

Definitions of Key Terms:

1. Information:
As per Section 2(f) of the RTI Act, "information" means any material in any form, including records, documents, emails, opinions, press releases, circulars, orders, logbooks, contracts, and any other information related to public authority.

2. Right:
The "right" refers to the entitlement of any citizen to seek information from public authorities as provided under the RTI Act. It includes the right to inspect documents, take copies, and obtain samples of materials held by public authorities.

3. Record:
"Record" refers to any document, manuscript, file, microfilm, microfiche, or any other material produced and held by a public authority.

4. Public Authority:
A public authority is defined in Section 2(h) of the Act as any government body or institution that is funded or controlled by the government. This includes:
- Central and State government offices
- Local authorities (municipalities, panchayats, etc.)
- Government-owned corporations and companies
- NGOs receiving substantial financial assistance from the government.

Obligations of Public Authorities:

1. Disclosure of Information:
Public authorities are required to proactively disclose certain information, including details about their organization, functioning, rules, and regulations, and financial disclosures.

2. Maintenance of Records:
Public authorities are required to maintain records in a manner that facilitates easy access and retrieval of information, ensuring transparency.

3. Appointment of PIOs:
Each public authority must designate Public Information Officers (PIOs) to handle information requests. PIOs must ensure timely responses to information requests.

4. Protection of Whistleblowers:
The Act also includes provisions for protecting individuals from any retribution when they expose corruption or wrongdoings by public authorities.

Requesting Information:

Filing a Request:
Citizens can request information by submitting a written or electronic application to the designated Public Information Officer (PIO) of the concerned public authority. The request must be clear and specific in terms of the information sought.

Fee Structure:
There is a nominal fee for filing a request, and the costs for providing copies of the information are prescribed under the Act.

Functions of Public Information Officer (PIO):

1. Processing Requests:
The PIO is responsible for receiving and processing RTI requests. They must provide information or acknowledge the receipt of the request within the time limits set by the Act.

2. Transfer of Requests:
If the information requested does not come under the jurisdiction of the PIO's authority, the PIO must transfer the request to the correct authority within five days of receipt.

3. Exemptions and Denials:
If a PIO decides that the requested information falls under an exemption, they must communicate this decision in writing, citing reasons for the denial, and inform the applicant of their right to appeal.

4. Appeals:
In cases where information is denied or delayed, the PIO is responsible for informing the applicant of their right to appeal to a higher authority within the same organization or to the Information Commission.

Information Technology Act, 2000
The **Information Technology Act, 2000** (IT Act) is India's primary law governing cyber activities. It was enacted to facilitate secure electronic transactions, recognize digital signatures, and address cybercrimes, providing a legal framework for e-commerce and digital governance.

Rationale Behind the IT Act, 2000

1. **Facilitate E-Commerce**:
    - With the rise of internet-based trade, the Act provided a legal foundation for recognizing electronic transactions and records.
2. **Legal Recognition of Digital Practices**:
    - Addressed the need for recognizing digital signatures, electronic records, and contracts as legally valid.
3. **Cybercrime Regulation**:

    - Introduced provisions to combat unauthorized access, hacking, data breaches, and other forms of cybercrime.
4. **Digital Governance**:
    - Enabled electronic delivery of government services to enhance efficiency and transparency in public administration.
5. **Compliance with International Standards**:
    - Aligned India's legal framework with the **United Nations Commission on International Trade Law (UNCITRAL)** model law on e-commerce

Digital Signature and Electronic Signature

Digital Signature

- **Definition**: A digital signature is an electronic method used to authenticate the identity of the sender and ensure the integrity of the message or document.
- **Technology**: Utilizes **asymmetric cryptography** with public and private keys.
- **Legal Validity**: Recognized under Section 3 of the IT Act, a digital signature ensures that:
    1. The document has not been altered after signing.
    2. The signatory's identity is verified.
- **Usage Examples**:
    - Filing income tax returns online.
    - Signing contracts digitally.

Electronic Signature

- **Definition**: A broader term that refers to any electronic method of signing, including digital signatures. It includes other authentication techniques like biometrics or OTPs.
- **Key Difference**: While all digital signatures are electronic signatures, not all electronic signatures are digital.
- **Legal Recognition**: Section 3A of the IT Act recognizes electronic signatures as valid, provided:
    1. They are reliable.
    2. The signatory can be identified.
    3. The document is unaltered after signing.

Aspect	Digital Signature	Electronic Signature
Definition	A cryptographic technique that uses a mathematical algorithm to validate the authenticity and integrity of a document.	A broad term encompassing any electronic method of signing a document, such as typing a name or using an OTP.
Technology Used	Based on **asymmetric cryptography** (public and private keys).	Can use various methods like typing, scanning signatures, OTPs, biometrics, or images of signatures.
Legal Basis in India	Explicitly recognized under **Section 3** of the IT Act, 2000.	Recognized under **Section 3A** of the IT Act, provided it is reliable and satisfies certain conditions.
Authentication Level	Provides a **high level of security** by verifying the signatory's identity and ensuring the document's integrity.	Generally **less secure** as it may not guarantee authenticity or prevent tampering.
Verification Process	Verified using a **Certificate Authority (CA)** that issues a Digital Signature Certificate (DSC).	Relies on simpler methods, such as email or SMS-based verification, without requiring a Certificate Authority.
Security Features	Ensures:	Offers:
	1. **Integrity**: Ensures the document hasn’t been altered.	1. Basic assurance of intent to sign.
	2. **Non-repudiation**: The signer cannot deny signing the document.	2. May or may not prevent tampering, depending on the method used.
Applications	High-security scenarios such as:	Routine applications where high security is not critical:
	- Filing tax returns (e.g., Income Tax, GST).	- Signing contracts, agreements, or consent forms.
	- E-commerce transactions requiring verified signatures.	- Approving documents or simple business workflows.
Examples	- DSC for filing in MCA (Ministry of Corporate Affairs).	- Scanned image of a handwritten signature.
	- Signing government forms (e.g., Aadhaar-based verifications).	- Clicking "I Agree" on terms and conditions.
Cost	More expensive as it involves acquiring a **Digital Signature Certificate** from a licensed Certifying Authority.	Less expensive as it often requires no additional infrastructure or specialized hardware.

Electronic Governance (E-Governance)

E-Governance refers to the use of digital tools to provide government services efficiently, transparently, and effectively. The IT Act facilitates e-governance through the following provisions:

1. **Legal Recognition of Electronic Records**:
   - Section 4 grants electronic records the same legal status as paper-based documents, enabling digitization of official processes.
2. **Acceptance of Electronic Signatures**:
   - Section 5 allows electronic signatures to authenticate electronic records in place of physical signatures.
3. **Filing and Retention of Electronic Documents**:
   - Section 6 enables filing, storage, and retrieval of government records electronically.
   - Example: Filing RTI applications or income tax returns online.
4. **Delivery of Services**:
   - Section 6A facilitates electronic delivery of services by government agencies, such as issuing digital certificates or licenses.
5. **Digitization of Governance**:
   - Promotes paperless governance through initiatives like Aadhaar, e-filing, and online public grievance portals.